Cisco Nexus Dashboard Insights Analysis Hub リリース 6.5.1 : Cisco ACI 向け

目次

初版：2024 年 7 月 23 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883

新規情報および変更情報

次の表は、最新リリースまでの主な変更点の概要を示したものです。ただし、本リリースまでの変更点や新機能の一部は表に記載されていません。

Cisco Nexus Dashboard Insights の新機能と変更された動作

特長	説明	リリース	参照先
バグ スキャンに含まれるバグ説明	バグ スキャンの [バグ（Bugs）] エリアのバグのテーブルに、各バグの説明が含まれるようになりました。	6.5.1	
テンプレート ベースのコンプライアンス ルールの機能拡張	この機能を使用すると、テンプレート内の特定のオブジェクトの状態を定義できます。STATUS は、オブジェクトが存在するかどうかにかかわらず、テンプレート内の特定のオブジェクトの状態を定義します。	6.5.1	コンプライアンスのタイプ
サステナビリティ レポートの上位 5 デバイス	サステナビリティ レポートでは、推定コスト、消費エネルギー、温室効果ガス（GHG）排出量の上位 5 デバイスが表示されます。	6.5.1	スイッチのサステナビリティ レポートの表示
Cisco ACI のトラフィック分析	Cisco ACI のトラフィック分析を使用できるようになりました。	6.5.1	トラフィック分析

電力マップの代わりに Cisco Energy Manager を活用	Nexus Dashboard Insights は、電力マップからではなく、Cisco Energy Manager からエネルギー コストと温室効果ガス（GHG）排出データを取得するようになりました。Cisco Energy Manager を使用すると、リージョンのシングルポイント障害やデータの欠落を回避することで、より堅牢なメソッドでデータを収集できます。	6.5.1	持続可能性レポート

特長	説明	リリース	参照先
接続分析の UI の機能拡張	接続分析 UI が再設計されました。	6.5.1	接続の分析
用語の変更	「サイト」という用語が「ファブリック」に名前変更されました。	6.5.1	ドキュメント全体

このドキュメントは、Nexus Dashboard Insights の GUI およびオンラインで www.cisco.com で入手できます。本書の最新バージョンに関しては、「Cisco Nexus Dashboard Insights 」の「Documentation」を参照してください。

コンプライアンス

コンプライアンス

[コンプライアンス（**Compliance**）**]** により、ユーザーは一連のルールを定義して、通信および構成の標準またはユーザーの予想を適用できます。

[管理（**Manage**）**]** > **[**ルール（**Rules**）**]** > **[**コンプライアンス ルール（**Compliance Rules**）**]** > **[**コンプライアンス ルールの作成（**Create Compliance Rule**）**]** の順に選択します。

ルール作成ページにアクセスする別の方法は、 分析ハブ の コンプライアンスで [コンプライアンスルールの作成（Create Compliance Rule）] ボタンをクリックすることです。これにより、ルールの作成に移動します。

ルールの状態は、作成後に変更できます。ルールが [有効（Enabled）] 状態の場合、次回の生成時にそのルールを使用してコンプライアンス レポートが生成されます。ルールが [無効（Disabled）] 状態の場合、そのルールは使用されません。

[構成（**Configure**）**]** > **[**ルール（**Rules**）**]** の順に選択し、テーブルの [ルールの状態（Rule State）] 列から特定のルールを有効または無効化にします。行の [アクション（Actions）] メニューをクリックし、**[**編集（**Edit**）**]** をクリックして **[**コンプライアンス ルールの編集（**Edit Compliance Rule**）**]** を開きます。**[**状態（**State**）**]** フィールドで、状態を **[**有効（**Enabled**）**]** に変更し、**[**保存（**Save**）**]** をクリックします。

コンプライアンスのタイプ

コンプライアンスには、通信コンプライアンスと構成コンプライアンスの 2 種類があります。 設定 タブを選択すると、ベスト プラクティスとビジネス要件を満たす構成を有効にして適用できます。

[通信（**Communication**）**]** を選択すると、ビジネスおよび規制目的を満たすネットワーク オブジェクト間の通信または分離が可能になります。コンプライアンス通信ルールを作成するには、「コンプライアンス 通信ルールの作成」を参照してください。

- 通信コンプライアンスは、次のコンプライアンス ルール タイプで構成されます。
  - サービス レベル契約（**SLA**）コンプライアンス：他のエンティティと通信する必要があるエンティティのルールを設定できます。コンプライアンス機能を使用して、規制コンプライアンスルールを設定できます。
  - **[**トラフィック制限コンプライアンス（**Traffic Restriction Compliance**）**]**：オブジェクト間の通信のプロトコルとポートに関する制限を指定できます。
  - **[**セグメンテーション コンプライアンス（**Segmentation Compliance**）**]**：他のエンティティと通信してはいけない一連のエンティティの周囲にファイアウォールで囲まれたエリアを確立できます。
- **[**構成コンプライアンス（**Configuration Compliance**）**]** を使用すると、指定した構成に対して構成コンプライアンス チェックを実行できます。

  構成コンプライアンスは、さらに次の 4 つのタイプに分類できます。

  - **[**スナップショット設定コンプライアンス（**Snapshot Settings Compliance**）**]**：これは、構成コンプライアンス チェックの方法に似ていますが、スナップショットも選択します。この方法を使用すると、スナップショット間を移動するときに、オブジェクトの特定の属性が変更されないようにできます。スナップショットを選択したコンプライアンス ルールを作成するには、「スナップショットを選択したコンプライアンス ルール の作成」を参照してください。
  - **[**手動構成（**Manual Configuration**）**]**：BD、VRF、EPG、コントラクト、サブジェクト、および

フィルタなど特定のオブジェクトにこれを構成できます。すべてのオブジェクトタイプがサポートされているわけではありません。手動構成でコンプライアンス ルールを作成するには、「手動構成でコンプライアンス ルールを作成する」を参照してください。

- **[テンプレート ベース コンプライアンス（Template based Compliance）]**：テンプレートベースのコンプライアンスを使用すると、任意の属性に基づいてオブジェクトを柔軟に選択し、他のコンプライアンスタスクの設定時にサポートされないさまざまなタイプの一致基準を提供できます。テンプレートベースのコンプライアンスを作成するには、「テンプレートベースのコンプライアンスの作成」を参照してください。

テンプレートベースのコンプライアンスにより、テンプレートを設定し、クエリのタイプを指定して、有効になっているときに特定の条件を適用するオブジェクトと属性を選択できます。テンプレートクエリ言語を使用すると、構成定可能なオブジェクトを選択し、コンプライアンスに適用する属性を定義できます。

他のタイプのコンプライアンス構成のリリースでは、JSON/XML ファイルをアップロードできます。ファイル内の属性はすべてそのまま一致します。または、名前の一致に基づいて特定のオブジェクトをいくつか選択し、それらのオブジェクトでサポートされる選択属性も設定できます。これにより、指定されたパラメータへのコンプライアンスをチェックする名前に一致する既存または将来のオブジェクトを検索できます。

+

- **[構成のコンプライアンスのインポート（Import Configuration Compliance）]**：指定した構成に対してインポート構成を実行できます。構成ファイルまたはスナップショットを指定すると、Cisco Nexus Dashboard Insights が継続的にチェックするため、Cisco APIC で定義されたオブジェクトと構成可能な属性の変更を識別できます。構成が指定した設定と異なる場合、違反が発生します。違反ごとに、個別の違反の異常が表示されます。さらに、違反ではないテナントのすべてのオブジェクトに対するすべての変数を含む単一の異常が発生します。インポート構成コンプライアンスを作成するには、「インポート構成コンプライアンスの作成」を参照してください。

コンプライアンスの例

- テンプレートベースのコンプライアンスの例
  - 以下は、テンプレートベースの設定コンプライアンスの例です。この例では、名前が **Ctrct_(1-3)** で始まるすべてのコントラクトを選択します。それから、**scope** を一致させます。これは **context** である必要があります。名前が any（ワイルドカード）で、**nameAlias** が ABC である必要があるコントラクト科目を選択します。**status MUST_EXIST** は、存在するすべての親ノードについて、少なくとも 1 つの obj_type が存在する必要があることを意味します。選択が定義されている場合は、その条件に従う必要があります。

```
{
  " vzBrCP" :
  {
    " attributes" :
    {
      " STATUS" : " MUST_EXIST" ,
      " SELECT(name)" : " REGEX(Ctrct_[1-3])" ,
      " MATCH(scope)" : " EXACT(context)"
    },
    " children" :
    [
      {
        " vzSubj" :
        {
```

```
        " attributes" :
        {
          " SELECT(name)" : " REGEX(.*)" ,
          " nameAlias" : " ABC"
        },
        " children" :
        [
          {
            " vzRsSubjFiltAtt" :
            {
              " attributes" :
              {
                " SELECT(tnVzFilterName)" : " ENDS_WITH(3_1_1)" ,
                " MATCH(action)" : " deny"
              }
            }
          }
        ]
      }
    }
  ]
 }
}
```

- BD には IPv4 サブネットと、特定のテナントに関連付けられた L3Out がありますか。これは、次のテンプレートで評価できます。

```
{
   " fvTenant" :
   {
      " attributes" :
      {
         " SELECT(dn)" : " OR(uni/tn-mgmt,uni/tn-tcam_comp_aepg_aepg,uni/tn-
Corp102)"
      },
      " children" :
      [
         {
            " fvBD" :
            {
               " attributes" :
               {
                  " SELECT(name)" : " REGEX(.*)"
               },
               " children" :
```

```
        [
          {
            "fvSubnet":
            {
              "attributes":
              {
                "SELECT(ip)":"REGEX(^[A-Fa-f0-9]{1,4}\\:*)",
                "ctrl":"nd",
                "ipDPLearning":"enabled",
                "scope":"public"
              }
            }
          },
          {
            "fvRsBDToOut":
            {
              "attributes":
              {
                "STATUS":"MUST_EXIST",
                "MATCH(tnL3extOutName)":"REGEX(L3Out_W02_[A-Za-z0-9])"
              }
            }
          },
          {
            "fvRsCtx":
            {
              "attributes":
              {
                "MATCH(tnFvCtxName)":"REGEX(VRF_W02_[A-Za-z]*)",
                "STATUS":"MUST_NOT_EXIST"
              }
            }
          },
          {
           "fvRsBDToNdP":
           {
             "attributes":
            {
              "STATUS":"MUST_EXIST"
            }
           }
         }
        ]
      }
    }
```

```
    ]
  }
}
```

- EPG に VMM ドメインが構成されていてはなりません。これは、次のテンプレートで評価できます。

```
{
   " fvTenant" :
   {
      " attributes" :
      {
         " SELECT(dn)" : " STARTS_WITH(uni/tn-NAE_contract)"
      },
      " children" :
      [
         {
            " fvAp" :
            {
               " attributes" :
               {
                  " SELECT(name)" : " REGEX(.*)"
               },
               " children" :
               [
                  {
                     " fvAEPg" :
                     {
                        " attributes" :
                        {
                           " floodOnEncap" : " disabled" ,
                           " hasMcastSource" : " no" ,
                           " MATCH(name)" : " REGEX(^EPG_W02_[A-Za-z0-9_-]*)" ,
                           " pcEnfPref" : " unenforced" ,
                           " prefGrMemb" : " include" ,
                           " MATCH(prio)" : " REGEX(^level[0-9])" ,
                           " shutdown" : " no"
                        },
                        " children" :
                        [
                           {
                              " fvRsDomAtt" :
                              {
                                 " attributes" :
                                 {
```

```
                                "instrImedcy": "lazy",
                                "resImedcy": "pre-provision",
                                "STATUS": "MUST_NOT_EXIST"
                            },
                            "children":
                            [
                                {
                                    "fvAEPgLagPolAtt":
                                    {
                                        "attributes":
                                        {
                                            "annotation": ""
                                        },
                                        "children":
                                        [
                                            {
                                                "fvRsVmmVSwitchEnhancedLagPol":
                                                {
                                                    "attributes":
                                                    {
                                                        "MATCH(tDn)":
"ENDS_WITH(LACP_SDN)"
                                                    }
                                                }
                                            }
                                        ]
                                    }
                                }
                            ]
                        }
                    }
                ]
            }
        }
    ]
  }
}
```

- テンプレートベースのコンプライアンスの無効な例
  - 次の*無効な*例では、**ABCXYZ** という名前の BD がある場合、**fvBD** の両方の子オブジェクト テンプレート スニペットによって選択されます。2 つの異なる選択とオブジェクトの検証を発生させる可能性があり、同じオブジェクト時間に対して基準を共存させることはできないため、

これは違反です。したがって、 **[**タイプ（**type**）**]** は **[**通常（**regular**）**]** または **[fc]** のいずれかです。

```
{
  " fvTenant" :
  {
    " attributes" :
    {
      " SELECT(name)" : " EXACT(tenantABC)"
    },
    " children" :
    [
      {
        " fvBD" :
        {
          " attributes" :
          {
            " MATCH(type)" : " EXACT(regular)" ,
            " SELECT(name)" : " REGEX(.*ABC.*)"
          }
        }
      },
      {
        " fvBD" :
        {
          " attributes" :
          {
            " MATCH(type)" : " EXACT(fc)" ,
            " SELECT(name)" : " REGEX(.*XYZ.*)"
          }
        }
      }
    ]
  }
}
```

コンプライアンス *ルール*

コンプライアンス ルールは、コンプライアンス違反またはコンプライアンスを満たす可能性のある異常を生成するために作成されます。コンプライアンス ルールを作成したら、コンプライアンス レポートを生成して、配置するとネットワークがどの程度ルールに適合しているかを確認できます。

[管理（**Manage**）**]** > **[***ルール*（**Rules**）**]** > **[***コンプライアンス ルール*（**Compliance Rules**）**]** の順にクリックします。ここには、作成されたすべてのルールが一覧表示されます。[コンプライアンス ルール（Compliance Rules）] ページでは、作成されたすべてのルールを 1 か所で表示できます。

このページでは、次の操作を実行できます。

- **[...]** ボタンを使用してルールを編集または削除する
- チェックボックスをクリックして複数のルールを選択し、まとめて削除/編集する
- **[**コンプライアンス *ルール*の作成（**Create Compliance Rule**）**]** ボタンから新しいルールを作成します。
- 次の属性による検索を使用してルールをフィルタリングします。
  - 名前
  - 説明
  - ルールタイプ
  - 状態
  - 最終変更日時
- ルールの概要を表示するスライドインを表示するには、ルールをクリックします。次の情報を表示します。
  - [全般（General）]：ルールの説明、ファブリック、および状態
  - [設定（Settings）]：ルール タイプ、ルールの作成に使用されるオブジェクト、および使用される構成コンプライアンス ルール 。
- **[**アクション（**Actions**）**]** では、ルールを編集、削除、無効化できます。

コンプライアンス *ルール*の解釈

次の表に、コンプライアンス ルールの例と、それらが作成する条件を示します。

コンプライアンスのルール	条件が作成されました
名前が "a" で始まり、"z" で終わるテナントの EPG が含まれます。	両方の基準を満たす "abz" などのテナント内の EPG は、1 回だけ含まれます。
名前が "a" で始まり、テナントが "xyz" で VRF インスタンス名に "c" が含まれる VRF インスタンスにもあるテナントの EPG が含まれます。	例：DN uni/tn-xyz/ctx-abcde の VRF インスタンスにあるテナント「abc」の下の EPG が選択されている場合、テナントと VRF インスタンスの両方の基準が一致することを確認します。DN uni/tn-xyz1/ctx-abcde を持つ VRF インスタンスにあるテナント "abc" の EPG は、VRF インスタンスのテナントが一致しないため選択されません。
"d" を含むものを除く、"a" で始まるテナントの下にあるすべての EPG が含まれます。	テナント "abc" の下の EPG は選択されていません。テナント "abcd" の下の EPG は選択されていません。
DN が uni/tn-rrr/ctx-sss の VRF インスタンスにもある EPG を除く、"a" で始まるテナントの下にあるすべての EPG が含まれます。	VRF インスタンスのテナントが一致するため、DN が uni/tn-rrr/ctx-sss の VRF インスタンスにあるテナント "abc" の下の EPG が選択されます。

コンプライアンス分析

ルールが変更された場合、または新しいルールが追加された場合は、バナーが表示されます。更新されたデータの分析を再実行できます。「変更済み」または「新規」タグは 、最近変更または追加されたルールの下に表示されます。

[アクション（**Actions**）**]** ボタンを使用すると、分析を再実行できます。

[概要（**Summary**）**]** には、違反の数、異常カウント別の上位ルール、違反による異常、およびルール タイプ別の違反が表示されます。[違反による上位ルール（Top rules by Violation）] のいずれかのルールをクリックして詳細を表示し、[違反からの異常の数（Number of anomalies from Violation）] の下のカウントをクリックして異常のリストを表示できます。

[違反からの異常（**Anomalies from Violations**）**]** には、作成されたルールによってトリガされたすべての異常が一覧表示されます。[グループ化（Grouped）] ビューでルールをクリックすると、そのグループに分類された異常のリストが表示されます。[グループ解除（Ungrouped）] ビューでルールをクリックすると、コンプライアンス ルールの詳細ページにリダイレクトされます。これは、すべてのファブリックのグループ ビューまたは特定のファブリックの個々のビューに表示できます。テーブルには、異常のシビラティ、異常をトリガしたルールのタイプ、検出時間、およびステータスが表示されます。

ルールをクリックすると、ルールの概要を示すスライドインが表示されます（問題点、 この異常をトリガした要因、 影響、 修正方法）

検索を活用して、アプリケーション プロファイル名、BD 名、カテゴリ、コンプライアンス オブジェクト名、コンプライアンス オブジェクト タイプ、コントラクト名、EPG 名、フィルタ名、L2 Out 名、L3 Out 名、レベル、ルール名、サブジェクト名、テナント名、VRF 名などの属性でフィルタします。歯車アイコンは、テーブルの列をカスタマイズするために使用されます。

[コンプライアンス *ルール*（**Compliance Rules**）**]** テーブルには、適用されたルールと違反したルールの概要が、各ルール タイプの数とともに表示されます。テーブルには、現在のレポートの生成に使用されたすべてのルールが一覧表示されます。テーブルには、構成ルールまたは通信ルールかどうか、および各ルールの違反による異常の数が示されます。

検索を活用して、名前、ルール タイプ、適用ステータス、検証済みなどの属性でフィルタ処理します。**[**コンプライアンス *ルール*の作成（**Create Compliance Rule**）**]** ボタンをクリックすると、ルール作成ページに移動します。

コンプライアンスの異常

UI でコンプライアンス ルールを指定すると、Cisco Nexus Dashboard Insights は後続のスナップショットで、コンプライアンス ルールが Cisco APIC で構成されたポリシーによって満たされているかどうかをを確認します。

発生する異常の数は、スナップショットに関連付けられたルールの数によって定義されます。たとえば、アシュアランス グループが 15 分ごとにスナップショットでコンプライアンス分析を実行し、スナップショットに 2 つのルールが関連付けられている場合、2 つの異常が発生します。

コンプライアンスの注意事項および制限事項

コンプライアンスの注意事項

- 1 つのコンプライアンス ルールを複数のファブリックに関連付けることができます。
- ファブリックごとに最大 30 のアクティブ通信コンプライアンス ルールと 600 のアクティブ構成コンプライアンス ルールを設定できます。この制限を超えると、**[**コンプライアンスの管理（**Manage Compliance**）**]** エリアに要件を追加できません。
- 1 つまたは複数のファブリックに対してコンプライアンス ジョブが進行中の場合、それらのファブリックのバグ スキャンを開始しないことを推奨します。

- ファブリック リストはいつでも変更できます。
- ルールの名前はファブリック全体で一意です。
- コンプライアンスは、次の Cisco APIC リリースでサポートされています。
  - 3.2(x) リリース
  - 4.0(x) リリース
  - 4.1(x) リリース
  - 4.2(x) リリース
  - 5.0(x) リリース
  - 5.1(x) リリース
  - 5.2(x) リリース
  - 5.3(x)リリース
  - 6.0(x) リリース

コンプライアンス ルールを作成するための注意事項

- コンプライアンス ルールを作成するときに、コンプライアンス違反の異常に表示されるカスタム説明を追加できます。
- コンプライアンス ルールはファブリック レベルで作成されます。
- コンプライアンス ルールは、オフラインまたはオンラインのいずれかです。

インポート構成コンプライアンスに関するガイドライン

- 新しい構成オブジェクトの追加を許可するには、このボックスをオンにします。これは、アップロードされた構成ファイルに欠落している新しいオブジェクトごとに違反を発生させます。

コンプライアンス ルールの命名の注意事項

- 名前は 3 文字以上にしてください
- 名前に特殊文字を含めることはできません
- 名前は一意である必要があります。
- 2 つのルールに同じ名前を付けることはできません。

テンプレートベースのコンプライアンスに関する検証済みの拡張性の制限

- テンプレート ルールの数は、構成可能なオブジェクトの総数が 150,000 の APIC の場合は 5 です。
- テンプレートごとに、平均して 15,000 個のオブジェクトを選択します。
- テンプレートあたりのテナント数は 30 テナントで、テナントごとに平均 500 個のオブジェクトを選択します。
- すべてのテンプレートで選択されたオブジェクトの総数が 5*15,000 未満であり、APIC 内の構成の総数が 150,000 オブジェクト未満の場合、5 つ以上のテンプレートを作成できます（ルールの上限は合計 30 です）。
- ファブリックごとに最大 30 のアクティブ通信コンプライアンス ルールと 600 のアクティブ構成コンプライアンス ルールを設定できます。

テンプレートベースのコンプライアンスの注意事項

- テンプレートには、APIC ファイルで使用される構造と同じ構造が使用され、オブジェクト、属性、および子があります。
- アップロードできるテンプレート ファイルのサイズは、空白を含めて最大 15 MB です。Pretty JSON ファイルには、インデントをサポートするための空白があります。ファイルサイズを小さくする場合、空白を削除してからファイルをアップロードしてください。
- テンプレートでは、コンプライアンスが属性に適用されるため、**attributes** の定義は必須です。
- テンプレートでは、**children** の定義は任意です。クエリに children が定義されている場合、選択内容は選択したオブジェクトの実際の children に適用されます。
- テンプレートでは、子配列ごとに 1 回だけ同じオブジェクトタイプを含めることができます。そうすることで、違反の異常を引き起こすコンプライアンスルールの競合につながる要件が作成される可能性を回避できます。
- 現在、JSON ファイルがサポートされています。XML ファイルはサポートされていません。
- アップロードできるテンプレートファイルのサイズは最大 15 MB です。ファイルサイズが 5 MB を超える場合、表示機能は使用できません。ファイルサイズが 5 MB を超える場合、ファイルをダウンロードして内容を表示できます。

コンプライアンス分析の制限事項

- オフライン分析に使用できるテレメトリはありません。
- **[**コンプライアンス ルール（**Compliance Rules**）**]** テーブルと **[**違反からの異常（**Anomalies from Violations**）**]** テーブルは、リリース 6.4(1) より前に生成されたレポートでは使用できません。テーブルを表示するには、分析を再度実行する必要があります。
- コンプライアンス レポートは 2 時間ごとに生成されます。

コンプライアンス通信ルールの作成

1. ルールの名前と説明を入力します。ルールを有効にするか無効化にするかを選択できます。
2. ルールを適用するファブリックを選択します。1 つ、複数、またはすべてのファブリックを選択できます。
3. [コンプライアンス ルール タイプ（**Compliance Rule Type**）] フィールドで、[通信（**Communication**）] を選択します。
4. **[**基準（**Criteria**）**]** の **[**通信タイプ（**Communication Type**）**]** フィールドで、適切な通信タイプを選択します。**[**要通信（**Must Talk To**）**]**、**[**通信不可（**Must Not Talk To**）**]**、**[**通信可（**May Talk To**）**]** などのオプションがあります。通信タイプは、2 つの異なるオブジェクト グループ間で適用されます。
5. **[**オブジェクト タイプ（**Object Type**）**]** フィールドと **[**トラフィック セレクタ（**Traffic Selector**）**]** エリアで、適切なオブジェクトとトラフィックセレクタを選択します。
6. 両方のグループに適切な基準を選択します。任意のオブジェクト タイプと対応する一致基準オブジェクトをセレクトします。使用可能なオブジェクト タイプと、さまざまな一致基準オブジェクトの定義方法については、「 一致基準 」を参照してください。
7. **[**基準の追加（**Add Criteria**）**]** エリアで基準を定義したら、**[**選択したオブジェクトの表示（**View Selected Objects**）**]** リンクをクリックして、選択したオブジェクトが適切であることを確認します。通信タイプとトラフィック セレクタ ルールの選択に基づき、定義したコンプライアンス ルールが表示されます。通信タイプとトラフィック セレクタの詳細については、「 通信コンプライアンス」を参照してください。

8. ファブリックに適したオブジェクト、基準、トラフィック制限を定義したら、ルール作成の概要全体を表示し、[ルールの保存（**Save Rule**）] をクリックして、構成を完了します。
9. ルールが保存されると、ポスト成功画面が表示されます。このページから、[コンプライアンス ビューの表示（**View Compliance rules**）]、[コンプライアンスの表示（**View Compliance**）]、または [別のコンプライアンス ルールの作成（**Create another Compliance rule** ）] を選択できます。

方向ベースのトラフィック設定を表示/編集するには、[方向（ **Direction**）] 設定列から確認します。

スナップショット選択でコンプライアンス ルールの作成

1. [コンプライアンス ルール タイプ（**Compliance Rule Type**）] で、[構成（**Configuration**）] を選択します。
2. [基本構成の設定（**Base Configuration Settings**）] フィールドで、[スナップショットの設定（**Snapshot Settings**）] を選択します。
3. [スナップショットの時間（**Time of Snapshot**）] フィールドで、目的のスナップショット時間を選択し、[適用（**Apply**）] をクリックします。
4. [新しいルール（**New Rule**）] で、[保存（**Save**）] をクリックします。Cisco Nexus Dashboard Insights がチェックの実行を開始します。
5. スナップショットをダウンロードするには、[設定（**Settings**）] の [ダウンロード（**Download**）] リンクをクリックします。

インポート構成コンプライアンスの作成

1. [コンプライアンス ルール タイプ（**Compliance Rule Type**）] で、[構成（**Configuration**）] を選択します。
2. [基本構成の設定（**Base Configuration Settings**）] フィールドで、[インポート構成（**Import Configuration**）] を選択します。JSON/XML ファイルをアップロードする場合、構成ルールは編集できません。そのような場合、ファイルをアップロード後、[アクション（**Actions**）] から移動して、ファイルを表示またはダウンロードできます。
3. アップロードするには、提供されたフィールドにファイルをドラッグ アンド ドロップします。[保存（Save）] をクリックします。

手動構成によるコンプライアンス ルールの作成

1. ルールの名前と説明を入力します。[有効（Enable）] または [無効（Disable）] の状態を選択できます。
2. ルールを適用するファブリックを選択します。1 つ、複数、またはすべてのファブリックを選択できます。
3. [コンプライアンス ルール タイプ（**Compliance Rule Type**）] フィールドで、[構成（**Configuration**）] を選択します。
4. [基本構成の設定（**Base Configuration Settings**）] フィールドで、[手動構成（**Manual Configuration**）] を選択します。
5. [オブジェクトの選択（Object Selection）] で、[オブジェクト タイプ（**Object Type**）] を選択し、必要に応じて基準を追加します。[選択したオブジェクトの表示（View Selected Objects）] ボタンを使用して、選択したオブジェクトを表示することもできます。任意のオブジェクト タイプと対応する一致基準オブジェクトを選択します。使用可能なオブジェクト タイプと、さまざまな一致基準オブ

ジェクトの定義方法については、「 一致基準 」を参照してください。属性の要件については、「手動構成の コンプライアンス」を参照してください。

6. 上記で選択した一致基準のルールをここに追加します。[ルールの追加（Add Rule）] をクリックし、ルールの属性、演算子、および値を選択します。

名前と名前のエイリアス属性の要件には、[正規表現に一致（Matches Regular Expression）] を選択する追加オプションがあります。

7. 作成するルールの概要全体を表示し、**[ルールの保存（Save Rule）]** をクリックします。Cisco Nexus Dashboard Insights は、指定した命名コンプライアンス要件に基づいてチェックの

実行を開始します。

8. ルールが保存されると、ポスト成功画面が表示されます。このページから、**[**コンプライアンス ビューの表示（**View Compliance rules**）**]**、**[**コンプライアンスの表示（**View Compliance**）**]**、または **[**別のコンプライアンス ルールの作成（**Create another Compliance rule** ）**]** を選択できます。

VRF に関連する BD の場合は、追加の要件が必要です。EPG 関連付けカウントを必要とする EPG 関連付け要件が追加されます。これは、
等しい 、 最低、 最高にできます。ただし、BD に [EPG 関連付け要件（Association Requirement）] または [（Name and Attribute Requirement）] のどちらかを追加するように選択できます。すべての属性を選択することはできません。「手動構成コンプライアンス」を参照してください。

テンプレートベースのコンプライアンスの作成

1. **[**基本構成の設定（**Base Configuration Settings**）**]** フィールドで、**[**テンプレートベースのコンプライアンス（**Template Based Compliance**）**]** を選択します。
2. **[**アップロードするファイルを選択またはドラッグアンドドロップ（**Choose a file or drag and drop to upload**）**]** エリアで、テンプレートベースのファイルをアップロードします。
3. ファイルのアップロードが完了したら、[表示]アイコンをクリックして、アップロードしたファイルの内容を確認できます。
4. **[**保存（**Save**）**]** をクリックします。

テンプレート シンタックスの詳細については、「オブジェクト セレクタを構成するためのテンプレート」を参照してください。テンプレートのオブジェクト セレクタを構成する方法については、「オブジェクト セレクタ を構成するためのテンプレート」を参照してください。

コンプライアンス分析のトリガ

[コンプライアンス分析（Compliance Analysis）] は、内部でアシュアランス分析をトリガし、コンプライアンス異常を生成します。

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**コンプライアンス（**Compliance Analysis**）**]** に移動します。
2. ドロップダウン メニューからファブリックを選択します。
3. レポートを表示する日付を選択します。

オブジェクト セレクタを構成するためのテンプレート

手動構成を使用して構成ルールを作成する場合、いくつかの特定のオブジェクト セレクタ（BD、EPG、VRF など）のみがサポートされます。テンプレートを使用すると、任意のオブジェクトを選択し、その属性に一致基準を適用できます。

オブジェクトは、Cisco APIC の任意の管理対象オブジェクトにすることができ、その選択はオブジェクトの識別名に基づきます。選択基準として別の属性を使用する場合は、そのオブジェクトの有効な属性を使用できます。タグと注釈に基づいて、選択基準と一致基準のオブジェクト セレクタを構成できます。

選択、ステータス、および一致基準

命名コンプライアンスの場合、コンプライアンス ルールは、**MATCH** によって示される [name] および

[nameAlias] フィールドにあります。

- **STATUS** は、オブジェクトが存在するかどうかにかかわらず、テンプレート内の特定のオブジェクトの状態を定義します。**STATUS** 基準は、次のいずれかのキーワードを使用して定義できます。
  - MUST_EXIST
  - MUST_NOT_EXIST

    以下はシンタックス例です。

```
{
" vzBrCP" :
 {
" attributes" :
  {
" STATUS" : " (<status selected>)" ,
" SELECT(name)" :" <KEY_WORD>(<value>)" ,
" MATCH(nameAlias/name)" :" <KEY_WORD>(<value>)"
  }
 }
}
```

- **SELECT** および **MATCH** 基準は、次のいずれかのキーワードを使用して定義できます。**MATCH** 基準は、コンプライアンス ルールを定義するために使用されます。**SELECT** では、オブジェクトのグループを選択するための基準を定義でき、 **MATCH** では、選択したオブジェクトが持つ必要がある属性と値を定義できます。コンプライアンスルールは、**SELECT** 基準を使用して選択されたオブジェクトに適用されます。
  - STARTS_WITH
  - ENDS_WITH
  - EXACT
  - OR
  - REGEX

    SELECT のシンタックス：

    SELECT(<attribute_name>): KEY_WORD(<value>)

    MATCH の構文：

    MATCH(<attribute_name>): KEY_WORD(<value>)

    Attribute_name には、オブジェクトの任意の属性を指定できます。REGEX(<value>) - 値は標準の正規表現シンタックス " SELECT(name)" : " REGEX(Ctrct_[1-3])" に従う必要があります。キーワードの正規表現の詳細については、「正規表現構造の概要」を参照してください。

    以下はシンタックス例です。

```
{
  " <object>" :
  {
    " attributes" :
    {
      " SELECT(dn)" :" <KEY_WORD>(<value>)" ,
      " MATCH(nameAlias/name)" :" <KEY_WORD>(<value>)"
    }
  }
}
```

属性に **SELECT** が指定されていない場合、**rn** と **dn** はデフォルトで **SELECT** と見なされます。

以下は、KEY_WORD が定義されていない場合の、デフォルトの動作が **EXACT**.であるシンタックス例です。MATCH(dn)および MATCH(rn)を使用すると、これらは一致基準として定義されます。

属性（**dn** および **rn** 以外）に **MATCH** または **SELECT** が指定されていない場合、デフォルトで **MATCH** と見なされます。

```
{
 " fvAEPg" :
 {
  " attributes" :
  {
   " SELECT(dn)" : " uni/tn-aepg_vzanycons_imd_ctx_pass_7/ap-CTX1_AP1/epg-
CTX1_BD1_AP1_EPG7" ,
   " MATCH(isAttrBasedEPg)" : " EXACT(no)" ,
   " prio" : " OR(unspecified, prio1)"
  }
 }
}
```

前述の例では、デフォルトで「prio」が **MATCH** になります。

[命名コンプライアンス（Naming Compliance）] を構成し、選択したオブジェクトが **name** または nameAlias に一致する
テンプレート名：

```
{
  " vzSubj" :
  {
    " attributes" :
    {
      " SELECT(dn)" :" EXACT(subj1)" ,
      " MATCH(nameAlias)" :" STARTS_WITH(ABC)"
```

```
    }
  }
}
```

属性 **dn** はデフォルトで常に **SELECT** と見なされ、他の属性は常に **MATCH** と見なされるため、前述のテンプレートは次の例のように簡略化できます。さらに、キーワードが定義されていない場合、デフォルトの動作は **EXACT** です。

```
{
  " vzSubj" :
  {
    " attributes" :
    {
      " dn" :" subj1" " nameAlias" :" STARTS_WITH(ABC)"
    }
  }
}
```

前述のテンプレートでは、" vzSubj" の代わりに任意のオブジェクトを使用でき、" dn" の代わりに任意の属性を使用できます。

・{} のテンプレート シンタックス

以下は、**KEY_WORD** が {} である汎用テンプレートのシンタックス例です。このテンプレートを使用して、要件のカスタマイズ、属性の選択、正規表現を行うことができます。

KEY_WORD の値は次のようになります。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

```
{
  " <MO type>" :
  {
    " attributes" :
    {
      " SELECT(<attribute>)" : " KEY_WORD(<expression>)" ,
      " MATCH(<attribute>)" : "  KEY_WORD (<value>)"
    },
    " children" :
    [
      {
```

```
      " <MO type>" :
      {
        " attributes" :
        {
          " SELECT(<attribute>)" : "  KEY_WORD (<value>)" ,
          " MATCH(<attribute>)" : "  KEY_WORD (<value>)"

        },
        " children" :
        [
          {
            " <MO type>" :
            {
              " attributes" :
              {
                " SELECT((<attribute>)" : "  KEY_WORD (<value>)" , " MATCH(<attribute>)" : "
                KEY_WORD (<value>,<value>)"

              }
            }
          }
        ]
      }
    }
  ]
 }
}
```

- 属性値が **NULL** または **EMPTY** のテンプレート

  以下は、属性値が null または空のテンプレートの例です。

```
" REGEX(^.{0}$)"
" EXACT()"
" OR(test, )"  <– use space
```

```
{
 " fvTenant" :
 {
   " attributes" :
   {
     " MATCH(annotation)" : " OR(orchestrator:msc, )" ,
     " SELECT(name)" : " REGEX(aepg_aepg_imd_tnt_pass_[0-9]+)" ,
   }
```

```
  }
}
```

前述のテンプレートを使用して命名コンプライアンスのオブジェクト セレクタを構成する手順については、「テンプレートベースのコンプライアンスの構成」を参照してください。

タグと注釈

APIC ユーザーとして、管理対象オブジェクト（MO）にタグを作成し、使用している APIC バージョンに基づいて、**tagInst** または **tagAnnotation** タイプの子オブジェクトを作成できます。

したがって、APIC で作成されたタグに基づいてオブジェクトを選択する場合は、このセクションで提供されるテンプレートに従い、タグと注釈に基づいてオブジェクトセレクタを設定できます。

子オブジェクトを **tagInst** タイプとして表示する例です。

```
{
  " <object>" :
  {
    " attributes" :
    {
      " MATCH(<attribute_name>)" :" <KEY_WORD(<value>)"
    },
    " children" :
    [
      {
        " <tagInst>" :
        {
          " attributes" :
          {
            " SELECT(<attribute_name>)" :" <KEY_WORD(<value>)"
          }
        }
      }
    ]
  }
}
```

子オブジェクトを **tagInst** タイプとして表示する例です。

```
{
  " <object>" :
  {
    " attributes" :
    {
```

```
        " MATCH(<attribute_name>)" :" <KEY_WORD(<value>)"
      },
      " children" :
      [
        {
          " <tagAnnotation>" :
          {
            " attributes" :
            {
              " SELECT(<key or value>)" :" <KEY_WORD(<value>)"
            }
          }
        }
      ]
    }
}
```

オブジェクトは、**tagAnnotation** または **tagInst** を子として持つ有効な APIC オブジェクトです。オブジェクトの選択は、**tagInst** の場合は名前、**tagAnnotation** の場合はキーまたは値に **SELECT** を使用して、**tagInst** または **tagAnnotation** オブジェクトで定義されます。

選択基準は、次のいずれかのキーワードです。

- STARTS_WITH
- ENDS_WITH
- EXACT
- OR
- REGEX

コンプライアンスルールは **MATCH** を使用して親オブジェクトレベルで定義され、基準は任意の **KEY_WORD** を使用して定義できます。 **tagInst** または **tagAnnotation** は選択基準のみを提供するため、コンプライアンス ルールには関係しません。

*タグが「BDs_in_cisco」であるすべての fVBD を **SELECT** するテンプレートの例を示します。BD の名前は **BD** または **app1BD** である必要があります。*

```
{
  " fvBD" :
  {
    " attributes" :
    {
      " MATCH(name)" :" OR(BD, app1BD)"
    },
    " children" :
    [
      {
```

```
        "tagInst":
        {
          "attributes":
          {
            "SELECT(name)":"EXACT(BDs_in_cisco)"
          }
        }
      }
    ]
  }
}
```

テンプレートを使用してタグと注釈に基づいてオブジェクトセレクタを構成する手順については、「テンプレートベース コンプライアンスの作成」を参照してください。

「テンプレートベース コンプライアンスの作成」の手順を使用してタグと注釈のオブジェクト セレクタを構成する場合は、追加の手順を実行する必要があります。**[保存（Save）]** をクリックする前に、**[新しいルールの作成（Create New Rule）]** ページで、**[tagAnnotation/tagInst に基づいたオブジェクト選択を有効にする（Enable Object Selection Based on tagAnnotation/tagInst）]** フィールドのチェックボックスをオンにする必要があります。したがって、いずれかのオブジェクトに tagAnnotation または tagInst がある場合、2 つのオブジェクトの選択基準に基づいて親が選択されます。

通信コンプライアンス

通信タイプ

- **[要通信（Must Talk To）]**：定義されたトラフィック制限ルールの下で、セレクタ B によって選択されたオブジェクトとセレクタ A が通信する必要があるオブジェクトを設定できます。
- **[通信不可（Must Not Talk To）]**：オブジェクト セレクタ *A によって選択されたオブジェクトが、定義されたタイプのトラフィックを使用して、オブジェクト セレクタ B によって選択されたオブジェクト*と通信しないようにする場合は、この構成を選択します。この設定では、トラフィック制限ルールはオプションです。

  このオプションを使用して、2 つの異なるタイプの通信コンプライアンスを設定できます。

  - [トラフィック制限コンプライアンス（Traffic Restriction compliance）]：セレクタ *A によって選択されたオブジェクトが、トラフィック制限ルールを使用する選択されたタイプのトラフィックを使用して、セレクタ B によって選択されたオブジェクト*と通信しないようにするトラフィック セレクタ ルールを指定できます。[この通信は制限されています。
  - [セグメンテーション コンプライアンス（Segmentation compliance）]：トラフィック セレクタ ルールを定義しないことで、セレクタ *A のオブジェクトがどのタイプのトラフィックを使用してもセレクタ B のオブジェクト*と通信できないセグメンテーション コンプライアンスを構成できます。この場合、ユーザーが定義するトラフィック制限ルールはありません。
- **[通信可]**：トラフィック制限コンプライアンスを作成できます。*セレクタ A によって選択されたオブジェクトは、トラフィック制限ルールを使用し特定のタイプのトラフィックのみを使用して、セレクタ B によって選択されたオブジェクトと通信できます。*

Nexus Dashboard Insights ユーザーとして、EPG A がトラフィック タイプ TCP IP を使用して EPG B と通信できることを確認するには、EPG A が TCP IP を使用して EPG B と通信可能なトラフィック制限ルー

ルを構成します。

通信タイプとトラフィック セレクタ ルールの選択と結果のコンプライアンス要件タイプ

通信タイプ	トラフィックセレクタルールの選択	選択できるオブジェクト	コンプライアンス要件タイプ
通話先	必須の選択肢	EPG	サービス レベル契約（SLA）
通話不可	必須でない選択肢	・EPG ・テナント	・[トラフィック セレクタ ルール（Traffic Selector Rule）] を選択した場合 コンプライアンス ルールはトラフィックの制限 ・[トラフィック セレクタ ルール（Traffic Selector Rule）] を選択しない場合、 [コンプライアンス ルール（Compliance Rule）] は、セグメンテーションです。
通話先	必須の選択肢	EPG	トラフィック制限

使用可能なトラフィック セレクタ ルール

イーサネット タイプ	プロトコルタイプ
ARP	-
FCOE	-
IP	・すべて ・EGP ・EIGRP ・ICMP ・ICMPV6 ・IGMP ・IGP ・L2TP ・OJPFIP ・PIM ・TCP ・UDP

MAC_SECURITY	-
MPLS_UNICAST	-
トリル	-

手動構成コンプライアンス

選択したオブジェクトに応じて設定できる属性要件

オブジェクト	関連付けられた属性
EPG	関連付けられた属性： ・**[優先グループ メンバー（Preferred Group Member）]**：優先グループメンバーは、*[含める（Include）]* または *[除外（Exclude）]* のいずれかと等しくても等しくなくてもかまいません。 ・**[インフラ EPG 分離（Infra EPG Isolation）]**：インフラ EPG 分離は、[非適用（Unenforced）]/[適用（Enforced）] と等しくても等しくなくてもかまいません。 ・**[QoS クラス（QoS Class）]**：QoS クラスは、未指定/レベル 1/レベル 2/レベル 3 と同等または同等ではありません。
VRF	関連付けられた属性： ・**[適用プリファレンス（Enforcement Preference）]**：適用プリファレンスは、[非適用（Unenforced）]/[適用（Enforced）] に設定できます。 ・**[適用方向（Enforcement Direction）]**：適用方向は、入力/出力と等しいか等しくないかを設定できます。 ・**[優先グループ（Preferred Group）]**：優先グループは、[無効（Disabled）]/[有効（Enabled）] に設定できます。 ・**[BD 適用（BD Enforcement）]**：BD 適用は、[はい（Yes）]/[いいえ（No）] に設定できます。

オブジェクト	関連付けられた属性
ブリッジドメイン（BD）	その属性は次のとおりです。 ・**[BD タイプ（BD Type）]**：BD タイプは、通常/FC に設定できます。デフォルト値は、regular と同等に設定されています。 ・**[L2 不明ユニキャスト（L2 Unknown Unicast）]**：これは、[フラッド（Flood）] または [ハードウェア プロキシ（Hardware Proxy）] と同じか、等しくないかのどちらかです。 ・**[L3 不明マルチキャストフラッディング（L3 Unknown Multicast Flooding）]**：これは、[フラッディング（Flood）]/[最適化されたフラッディング（Optimized Flood）] に設定できます。 ・**[BD マルチ宛先フラッディング（BD Multi Destination Flooding）]**：これは、BD で [カプセル化（Encapsulation）]/[ドロップ（Drop）]/[フラッド（Flood）] の [フラッド（Flood）] に設定できます。 ・**[PIM]**：[有効（Enabled）]/[無効（Disabled）] と同じまたは違うように設定できます。 ・**[ARP フラッディング（ARP Flooding）]**：[はい（Yes）]/[いいえ（No）] に設定できます。 ・**[IP ラーニングをサブネットに制限（Limit IP Learning to Subnet）]**：[はい（Yes）]/[いいえ（No）] に設定できます。 ・**[ユニキャストルーティング（Unicast Routing）]**：[はい/いいえ（Yes/No）] または [いいえ（Yes/No）] に設定できます。 ・[サブネット（Subnets）]：**[すべて（All）]/[なし（None）]/[少なくとも 1 つは共有（共有）]/[プライベート（Private）]/[パブリック（Public）]** に設定できます。

BD と EPG 間の関係の構成

この機能を使用すると、固定数の EPG を持つ BD セレクタを指定できます。BD コンプライアンスルールを設定することで、BD を関連付けられる EPG の最大数を設定できます。

このコンプライアンスルールの結果として、要件セットが満たされていない場合、違反の異常が発生します。要件が満たされている場合、適用異常が発生します。BD セレクタが解決されていない場合のみ、警告異常が発生します。

ユーザーは、指定された数の EPG が BD に関連付けられていることを確認するための要件を設定できます。この要件でサポートされている演算子は、**At least /At most /Equal to** です。たとえば、BD に少なくとも 5 つの EPG が関連付けられている必要がある要件が設定されており、BD に関連付けられている EPG が 5 未満（0 ~ 4）の場合、違反の異常が発生します。ただし、BD に 5 個以上の異常がある場合は、強制異常が発生します。

一致基準

選択したオブジェクト タイプの一致基準として使用可能なオブジェクト

オブジェクトタイプ	一致基準オブジェクト
EPG	・テナント ・VRF ・BD ・EPG ・アプリケーション プロファイル ・L3 Out ・L3 InstP ・L2 出力 ・L2 InstP
テナント	・テナント
BD	・テナント ・VRF ・BD
VRF	・テナント ・VRF
コントラクト	・テナント ・コントラクト
サブジェクト	・テナント ・情報カテゴリ
フィルタ	・テナント ・情報カテゴリ ・フィルタ

一致基準オブジェクトの定義

一致基準オブジェクト タイプ **1**	定義方法
テナント	tn - **operator** *value* **Object type 2**（VRF または BD のいずれか） a.[VRF] を選択した場合、ルールはさらに次のように定義されます。tn - **operator** *value* ctx - **operator** *value* a. [BD] を選択した場合、ルールはさらに次のように定義されます。 tn - **operator** *value* bd - **operator** *value*
VRF	tn - **operator** *value* ctx - **operator** *value*

BD	tn - **operator** *value* bd - **operator** *value*
一致基準オブジェクト タイプ **1**	定義方法
EPG	tn - **operator** *value* ap - **operator** *value* epg - **operator** *value*
アプリケーション プロファイル	tn - **operator** *value* ap - **operator** *value*
L3 Out	tn - **operator** *value* out - **operator** *value*
L3 InstP	tn - **operator** *value* out - **operator** *value* instp - **operator** *value*
L2 Out	tn - **operator** *value* l2out - **operator** *value*
L2 InstP	tn - **operator** *value* l2out - **operator** *value* instp - **operator** *value*
コントラクト	tn - **operator** *value* brc - **operator** *value*
件名	tn - **operator** *value* brc - **operator** *value* subj - **operator** *value*
フィルタ	tn - **operator** *value* flt - **operator** *value*

operator and *value* can be set to anything.

カスタム定義の演算子

演算子	説明
次の値と等しくなければなりません	この演算子は、指定された値の完全一致を返します。
次の値と等しくない	この演算子は、同じ値を持たないすべてを返します。
次を含む必要がある（Must Contain）	この演算子は、指定された値を含むすべてを返します。
次を含むことはできません:	この演算子は、指定された値を含まないすべてを返します。
次で始まる必要があります:	この演算子は、指定された値で始まるすべての値を返します。
次で終了する必要があります:	この演算子は、指定された値で終わるすべての値を返します。
次で始まることはできません:	この演算子は、指定された値で始まらないすべての値を返します。
次で終わることはできません:	この演算子は、指定された値で終わらないすべての値を返します。

適合性レポート

適合性レポート

適合性レポートでは、ネットワークのハードウェアおよびソフトウェアのライフサイクルを可視化し、理解できます。これは、アップグレードとハードウェアの更新を計画するのに役立ちます。適合性レポートは、ハードウェアおよびソフトウェアの適合性についてはファブリックごとに毎日、スケールの適合性についてはファブリックごとに毎週作成されます。レポートでは、ソフトウェア、ハードウェア、ソフトウェアとハードウェアの組み合わせ、ファブリックのスケールの適合性ステータスを確認することができます。

適合性レポートを活用し、既知の EoS および EoL 通知に対してネットワークでソフトウェアおよびハードウェア インベントリの現在のステータスを確認し今後の見通しを予測して、適合性を確認します。オンボード ファブリックのスケール適合性ステータスもモニタできます。

適合性レポートを使用すると、次のことができます。

- 販売終了（EoS）またはサポート終了（EoL）スイッチを実行するリスクを最小限に抑えます。
- 既知の EoS および EoL 通知に対してネットワークでソフトウェアおよびハードウェア インベントリの現在のステータスを表示して、適合性を確認します。
- ネットワーク内のソフトウェアおよびハードウェアのインベントリの将来的な見通しを予測します。
- オンボード ファブリックのスケール適合性ステータスをモニタします。

適合性レポートは、選択されたファブリックのソフトウェア、ハードウェア、およびスケールの適合性ステータスの概要を表示します。

適合性レポートでは、ハードウェアおよびソフトウェアの場合、適合スイッチはソフトウェアのリリースまたはハードウェアのプラットフォーム EoL の日付および PSIRT の終了日に基づき、3 つの重大度に分類されます。重大度には次のものがあります。

- [重大（Critical）] : PSIRT 終了日または最終サポート日が過去に発生しました。
- [注意（Warning）] : ソフトウェア リリースの EoL 日付またはハードウェア リリースの EoS が過去に発生しました。
- [正常性（Healthy）] : PSIRT 終了日、または サポート終了日、および EoL 日、またはソフトウェア リリースあるいはハードウェア リリースの EoS が将来発生する、またはソフトウェア リリースの EoL、ハードウェア リリースの EoS が発表されません。

販売終了およびライフサイクル終了のお知らせにあるソフトウェアメンテナンスリリースの終了日、および PSIRT の終了日は、インベントリをクリティカル、警告、または正常のカテゴリに分類するための参照マイルストーンとして使用されます。

適合性レポートでは、ファブリックのスケール適合性ステータスは、該当する場合、スイッチおよびコントローラで実行しているソフトウェア バージョンの Cisco の検証済みスケーラビリティ ガイドラインに基づいています。重大度には次のものがあります。

- 適合：すべてのメトリック値が 90%未満です。
- 到達制限：1 つ以上のメトリック値が 90% ~ 100%です。

・違反制限：1 つ以上のメトリック値が 100%を超えています。

適合性レポートへのアクセス

[分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**適合性

（**Conformance**）**]** に移動します。ドロップダウンリスト

から [ファブリック（Fabric）] を選択します。

または

[管理（**Manage**）**]** > **[**ファブリック

（**Fabrics**）**]** に移動します。ファブ

リックを選択します。

[全般（General）] セクションで、[適合性

（**Conformance**）**]** をクリックします。**[**レポー

トの表示（**View Report**）**]** をクリックします。

適合性レポートの表示

ブラウザ印刷オプションがある PDF として適合性レポートを保存できます（Chrome および Firefox でのみサポート）。

1. [適合レポート（Conformance Report）] に移動します。「適合性レポートへのアクセス」を参照してください。
2. ドロップダウン メニューからファブリックまたは **[**すべてのファブリック （**All Fabrics**）**]**を選択します。
3. ドロップダウン メニューから当月または前月を選択します。前月のレポートが使用可能な場合にのみ、前月を選択できます。

   適合性レポートには、適合性の概要、ハードウェアとソフトウェアの適合性、およびスケール適合性が表示されます。

4. [概要（Summary）] ページには、ハードウェアの適合性ステータス別のデバイス、ソフトウェアの適合性ステータス別のデバイス、ファブリックまたはスイッチのスケールの適合性ステータスが表示されます。詳細については、**[**適合基準の表示（**View Conformance Criteria**）**]** をクリックしてください。
5. [ハードウェア（Hardware）] または [ソフトウェア（Software）] ページには、適合性ステータス、適合性の見通し、デバイスの詳細が表示されます。
   a. [適合性見通し（Conformance Outlook）] セクションで、**[**全体（**Overall**）**]**、**[**ソフトウェア（**Software**）**]**、または **[**ハードウェア（**Hardware**）**]** をクリックして、ソフトウェアとハードウェア、ソフトウェアのみ、またはハードウェアのみの適合性を表示します。
   b. [デバイスの詳細（Device Details）] リストで、ハードウェアおよびソフトウェアの詳細を説明します。

c. ハードウェアの詳細には、デバイス名、ファブリック名、ハードウェア適合性ステータス、モデル、ロール、特定のデバイスの脆弱性サポート終了ハードウェアが含まれます。デバイス名をクリックして、追加の詳細を表示します。

d. ソフトウェアの詳細には、デバイス名、ファブリック名、ソフトウェア適合性ステータス、モデル、ソフトウェア バージョン、ロール、特定のデバイスの脆弱性サポート終了ソフトウェアが含まれます。デバイス名をクリックして、追加の詳細を表示します。

e. 検索を使用して、デバイス、ファブリック、ハードウェア適合性ステータス、ソフトウェア適合性ステータス、モデル、ソフトウェア バージョン、およびロールなど属性別にフィルタします。

f. 歯車アイコンを使用して、テーブルの列をカスタマイズします。

6. [スケール（Scale）] ページには、すべてのファブリックの概要、スケール適合性、およびスケール メトリックが表示されます。

a. [すべてのファブリックの概要（All Fabrics Summary）] セクションには、全体的なスケール適合レベル、拡張性メトリック違反による上位 5 つのスイッチ、コントローラとスイッチの拡張性メトリック、および拡張性メトリック違反の合計が表示されます。

b. 詳細については、**[適合基準の表示（View Conformance Criteria）]** をクリックしてください。

c. [スケール適合性（Scale Conformance）]セクションには、過去 6 ヵ月間のコントローラとスイッチのスケール適合性が表示されます（前の月のスケール レポートが使用可能な場合）。

d. [すべてのスケール メトリック（All Scale Metrics）] セクションには、ファブリックとスイッチのスケール メトリックの詳細が表示されます。ドロップダウン メニューから **[すべてのファブリック（All Fabrics）]** を選択すると、[すべてのスケール メトリック（All Scale Metrics）] セクションが表示されます。

i. ファブリックの詳細には、ファブリック名、タイプ、ソフトウェア バージョン、コントローラ メトリクス適合性、スイッチ メトリクス適合性を含みます。ファブリック名をクリックして、追加の詳細を表示します。

ii. スイッチの詳細には、スイッチ名、ファブリック名、ソフトウェア バージョン、モデル、転送スケール プロファイル、メトリクス適合性などが含まれます。スイッチ名をクリックすると、追加の詳細が表示されます。

iii. 検索を活用して、ファブリック、タイプ、ソフトウェアバージョンなどの属性でフィルタ処理します。

iv. 歯車アイコンを使用して、テーブルの列をカスタマイズします。

e. [ファブリック レベル スケール メトリック（Fabric Level Scale Metrics）] および [スイッチ レベル スケール メトリック（Switch Level Scale Metrics）] では、ファブリックおよびファブリックに関連付けられているスイッチのスケール メトリックを表示します。ドロップダウン メニューからファブリックを 1 つ選択すると、これらのセクションが表示されます。

i. ファブリックの詳細には、メトリック、適合性ステータス、およびリソースの使用状況が含まれます。

ii. スイッチの詳細には、スイッチ名、ファブリック名、ソフトウェア バージョン、モデル、転送スケール プロファイル、メトリクス適合性などが含まれます。スイッチ名をクリックすると、追加の詳細が表示されます。

7. [アクション（Actions）] メニューから、**[レポートの実行（Run Report）]** をクリックして、オンデマンド レポートを実行します。

ポリシー CAM

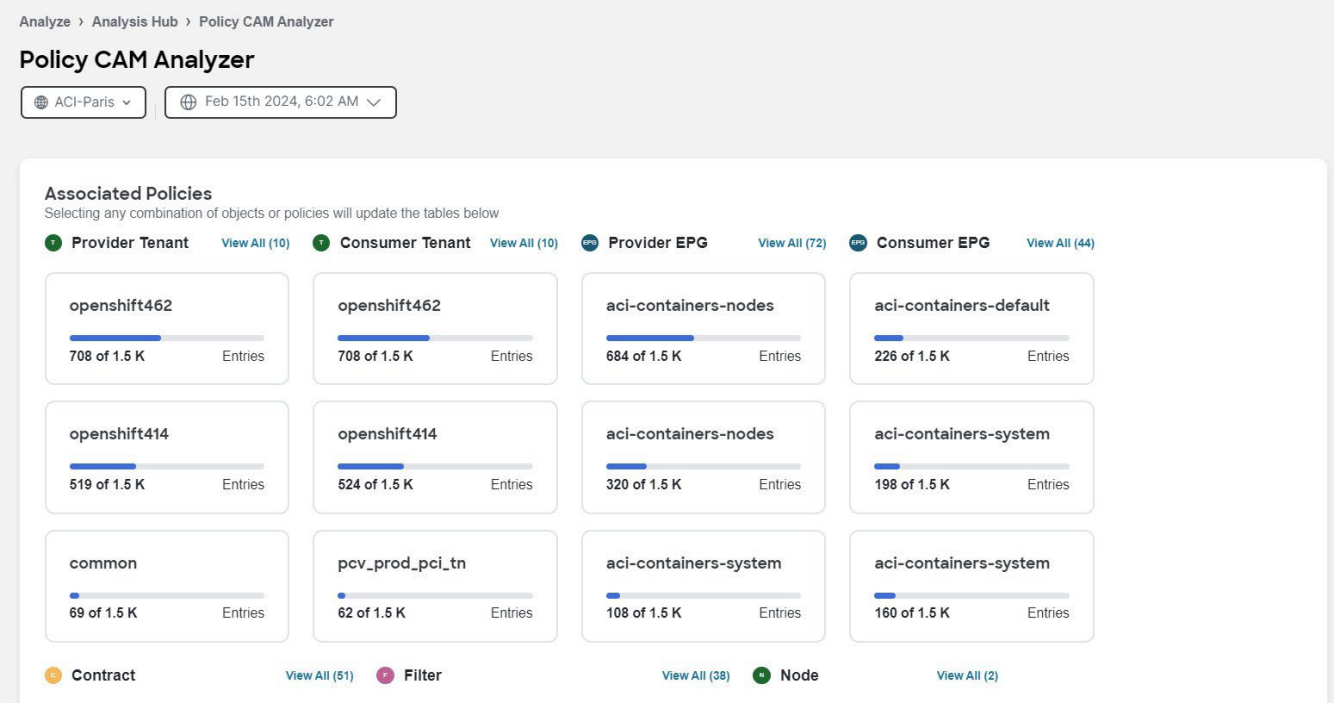
ポリシー CAM について

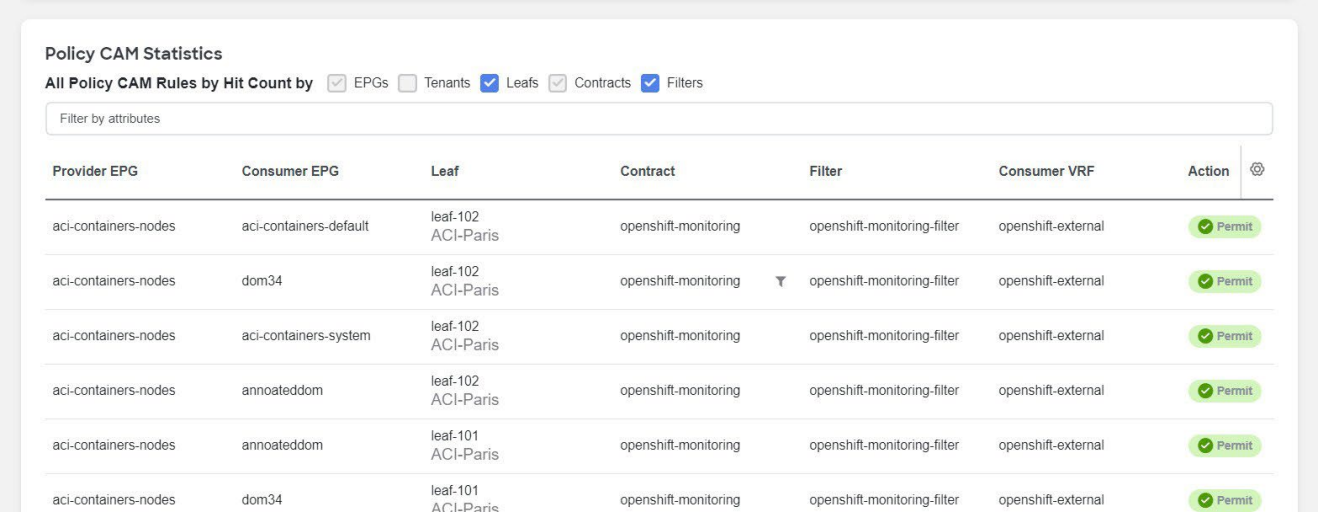
ポリシーCAM 機能は、ファブリック内のリソースの使用方法と使用場所を決定します。ポリシー CAM は、ネットワーク内のリソース使用率と、ポリシー連想メモリ（ポリシー CAM）使用率の量に関する情報を提供します。

[分析（Analyze）] > [分析ハブ（Analysis Hub）] > [ポリシー CAM（Policy CAM）] の順に選択します。

[ポリシー CAM（Policy CAM）] に移動したら、ファブリックを選択し、リソース使用率を表示する時間の適切なスナップショットを選択し、**[適用（Apply）]** をクリックします。

選択した時間範囲内で、最後のスナップショットは、ファブリックに含まれる ファブリックのそれぞれが考慮されます。したがって、選択した時間範囲内のアプリケーションの最新の状態を取得できます。





Policy CAM Analyzer には、次の情報が表示されます。

- 関連するポリシー
- ポリシーCAM 統計情報
- ポリシーCAM ルール
- すべての異常

Nexus Dashboard Insights リリース 6.3.1.15 では、ポリシー CAM は Cisco Nexus 9300-FX/FX3 スイッチでサポートされます。Nexus Dashboard Insights リリース 6.3.1.40以降は ポリシー CAM は Cisco Nexus 9000 FX3 スイッチでサポートされています。

関連するポリシー

関連付けられたポリシーには、使用可能なさまざまなオブジェクトまたはポリシーが一覧表示されます。ポリシーを上から下に表示すると、リストは最大使用率を持つノードから始まり、次に低い使用率が続きます。各列の各項目を選択して、テナント、コントラクト、EPG 間の関連付けと関係を表示できます。

[すべて表示（**View All**）] をクリックして、選択したオブジェクトのすべて

のノードをサイドパネルに表示します。次のオブジェクトまたはポリシーを

使用できます。

- プロバイダーテナント
- コンシューマテナント
- プロバイダーEPG
- コンシューマ EPG
- コントラクト
- フィルタ
- ノード

関連するすべてのオブジェクトとポリシーを表示するには、いずれかのオブジェクトをクリックします。

ポリシー**CAM** 統計情報

[ポリシー CAM 統計情報（Policy CAM Statistics）] テーブルには、すべてのノードと関連するルールが表示され、特定のノードの詳細にドリルダウンできます。テーブルに表示するオブジェクトのチェックボックスをクリックします。

次のオブジェクトを使用できます。

- EPG
- テナント
- リーフ
- コントラクト
- フィルタ

次の属性に基づいてテーブルをフィルタできます。

- プロバイダーEPG
- コンシューマ EPG
- リーフ
- コントラクト
- フィルタ
- コンシューマ VRF
- アクション

このテーブルには、次のタイムラインのヒット数も表示されます。

- 1 ヵ月
- 1 週間
- 1 時間
- 累計

歯車アイコンを使用すると、ビューごとに列を切り替えてテーブルをカスタマイズできます。

ポリシー**CAM** *ルール*

[ポリシー **CAM** *ルール*（**Policy CAM Rules**）**]** テーブルでは、選択したスナップショットに基づいてすべてのノードのリストを表示できます。

次の属性に基づいてテーブルをフィルタできます。

- リーフ
- プロバイダーEPG
- コンシューマ EPG
- コントラクト
- フィルタ
- ルール
- プロバイダ テナント名
- コンシューマ テナント名
- コンシューマ VRF

[ルール（Rules）] テーブルには、次の詳細情報が表示されます。

- リーフ
- プロバイダーEPG
- コンシューマ EPG
- コントラクト
- フィルタ
- ルール
- 有効なハードウェアエントリ数

- プロバイダ テナント名
- コンシューマ テナント名
- コンシューマ VRF

歯車アイコンを使用すると、ビューごとに列を切り替えてテーブルをカスタマイズできます。

すべての異常

[異常（Anomalies）] テーブルでは、選択した時間のスナップショットで生成された異常を、ノードごとに個別に、または集約して表示できます。

次の異常に基づいてテーブルをフィルタできます。

- 異常レベル
- アプリケーション プロファイル名
- 接続可能アクセス エンティティ プロファイル名
- BD 名
- 具象デバイス
- 具象インターフェイス
- コンシューマ アプリケーション プロファイル名
- コンシューマ EPG 名
- 契約
- 契約名
- デバイスクラスタ
- デバイス クラスタ インターフェイス
- デバイス選択ポリシー
- EPG 名
- VLAN のカプセル化
- ファブリック IP
- フィルタ名
- インターフェイス ポリシー グループ名
- 内部/外部
- L2 出力名
- L3 出力名
- リーフ インターフェイス プロファイル名
- リーフプロファイル名
- 論理インターフェイス コンテキスト
- 物理ドメイン名
- プロバイダー アプリケーション プロファイル名
- プロバイダーEPG 名

- プロバイダーテナント名前
- ルール名（Rule Name）
- ファブリック
- スパイン名
- テナント名
- 仮想ポート チャネル

接続の分析

接続の分析

接続分析を使用すると、2 つの異なるエンドポイント間のフローを分析して、エンドポイントがどのように接続されているかを把握し、問題が発生している可能性のある場所を特定できます。

接続性分析は、特定のフローについてネットワーク内の問題のあるノードを検出して分離するものであり、次の機能を備えています。

- 送信元から宛先エンドポイントまでの特定のフローについて、考えられるすべての転送パスをトレースします。
- 問題のあるデバイスを特定し、フローをドロップさせます。
- 転送パス チェックの実行、整合性チェッカーによるソフトウェアおよびハードウェア状態のプログラミングの整合性、パケット ウォークスルーに関する詳細など、問題の根本原因を絞り込むのに役立ちます。

接続分析オプション

Embedded Logic Analyzer Module (ELAM) : ELAM は、イーサネット トラフィック フローのトラブルシューティングに役立つ診断ツールです。アクティブフローからパケットをキャプチャし、イーサネットフレームのパケットドロップを分析します。ELAM では、送信元ホストと宛先ホスト間のアクティブフローが必要です。このオプションを有効にして、利用可能なアクティブ フローを分析できます。

[接続分析（Connectivity Analysis）] で実行されるチェックは次のとおりです。

- 全体的な正常性、リーフ スイッチ、スパイン スイッチ、リモート リーフ スイッチの接続などのトポロジ チェック
- エンドポイントの VRF および BD マッピング
- PC、VPC、 SVI 、ブレークアウト、SubIf などのインターフェイス接続
- ルーティング テーブル、EPM、および EPMC テーブル
- L3Out 情報とマッピング
- 隣接関係（ARP）テーブル
- トンネル情報
- スパイン スイッチの合成ルート（COOP）テーブル

注意事項と制約事項

- ファブリックごとに最大 10 個のジョブを送信できます。
- どの時点でも、ファブリックごとに 1 つの接続分析ジョブのみを実行できます。キューのジョブを停止し、別のジョブを実行できます。
- 接続分析機能は、Cisco APIC リリース 6.0(2h) および Cisco ACI スイッチ リリース 16.0(2h) 以降でサポートされています。Cisco Nexus Insights Cloud Connector （NICC）アプリケーション バージョン 3.0.0.350 は、Cisco APIC リリース 6.0(2h) に事前にパッケージ化されており、この機能に必要です。NICC の最新リリースが使用可能な場合は、**[**新しいバージョンを更新できます（**New version is available for update**）**]** バナーが表示されます。最新バージョンへの更新を推奨します。

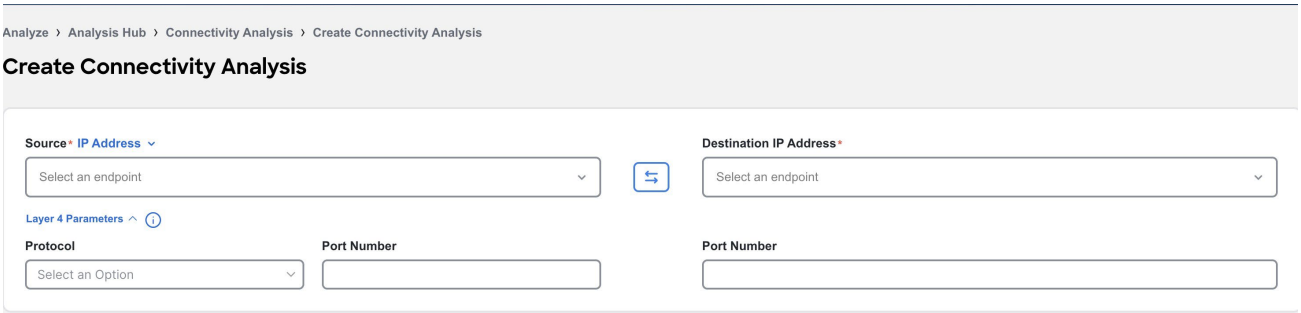
- オンライン ファブリックでのみ [接続性分析（Connectivity Analysis）] を実行できます。

サポートされるトポロジ

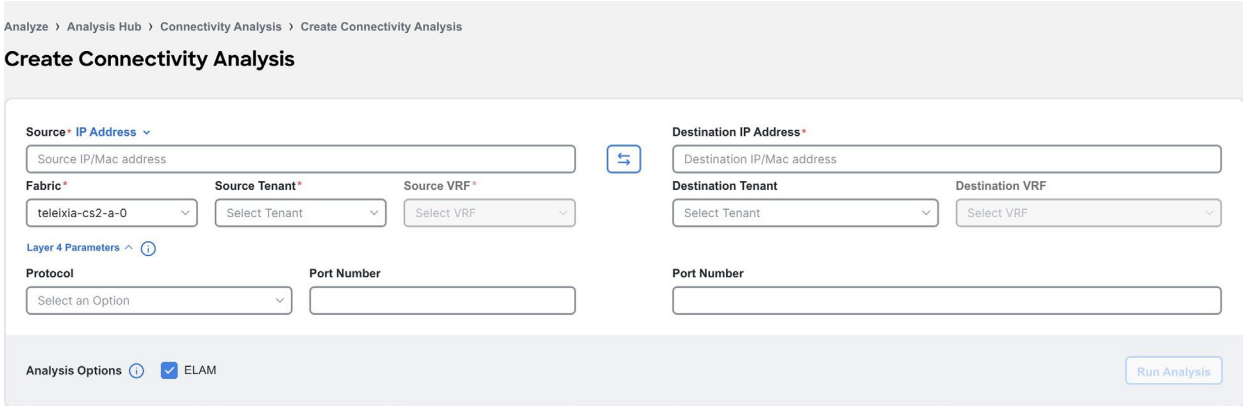
- エンドポイントの組み合わせ：
  - EP-EP
  - EP-L3Out
  - L3Out-EP
  - L3Out-L3Out
- 変換タイプ：
  - L2、L3、L4（TCP/UDP）
  - V4 および V6 のサポート
  - 移動およびプロキシ フロー
  - 共有サービス
- トポロジ：
  - シングルポッドとマルチポッド
  - リモート リーフダイレクト
  - M-Topology（ストレッチ ファブリック設計）
  - vPC
  - 3 階層アーキテクチャ

接続性分析の作成

1. **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[接続性分析（Connectivity Analysis）]** に移動します。
2. **[接続性分析の作成（Create Connectivity Analysis）]** をクリックします。



3. レイヤ 2 およびレイヤ 3 パラメータについては、次のように入力します。
   a. [送信元（Source）]ドロップダウン リストから、2 つのエンドポイント間のフローを分析する **IP** アドレスまたは **MAC** アドレスを選択します。
   b. ドロップダウン リストから送信元エンドポイントを選択するか、エンドポイントを入力します。一度に最大 20 個の IP アドレスまたは MAC アドレスを表示します。
   c. レイヤ 2 およびレイヤ 3 パラメータを手動で入力することもできます。**[詳細を手動で編集（Edit Details Manually）]** をクリックして、送信元 IP または MAC アドレス、宛先 IP または MAC アドレス、ファブリック タイプ、送信元テナント、送信元 VRF、宛先テナント、および宛先 VRF を入力します。



d. [宛先（Destination）]ドロップダウン リストから、2 つのエンドポイント間のフローを分析する IP アドレスまたは MAC アドレスを選択します。

e. ドロップダウン リストから宛先エンドポイントを選択するか、宛先エンドポイントを入力します。

4. レイヤ 4 パラメータに対して、以下を入力します。

   a. [プロトコル（Protocol）] ドロップダウン メニューから、[TCP] または [UDP] を選択します。

   b. 送信元ポートと宛先ポート番号を入力します。

5. [分析オプション（Analysis Option）] を選択します。

   a. [ELAM] オプションを有効にして、利用可能なアクティブ フローを分析できます。

6. [分析の実行（Run Analysis）] をクリックします。

7. [接続分析（Connectivity Analysis）] が完了すると、分析が **[Connectivity Analysis Jobs**（接続分析ジョブ）**]** テーブルに表示されます。**[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続性分析（**Connectivity Analysis**）**]** に移動して、[接続分析ジョブ（Connectivity Analysis Jobs）] ジョブを表示します。[分析（Analysis）] は、デフォルト名が割り当てられ、分析の名前を変更できます。

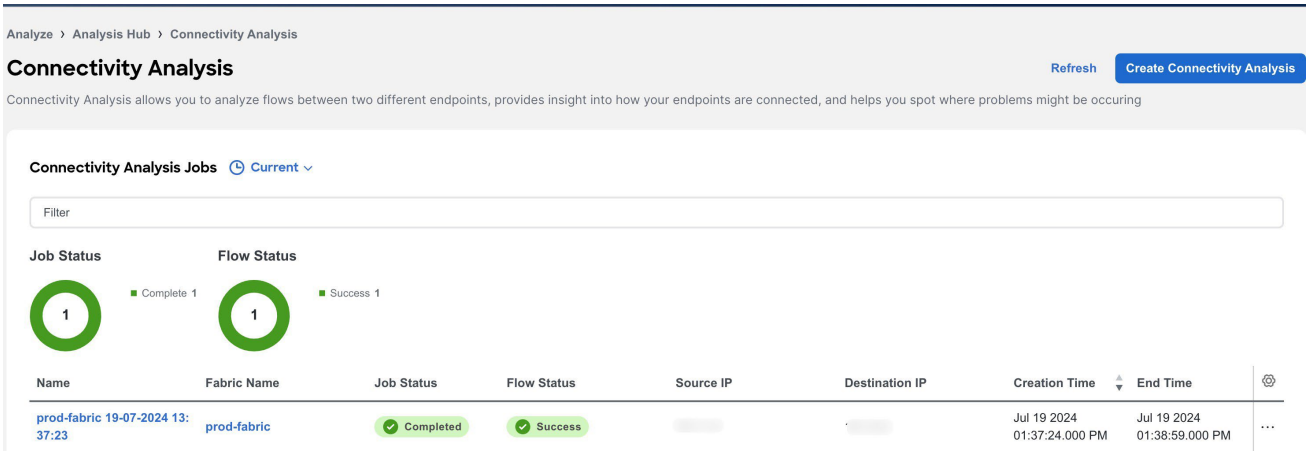
   a. 分析を選択し、[アクション（Actions）] ドロップダウン メニューから **[**分析の名前変更（**Rename Analysis**）**]** をクリックして名前を変更します。

または

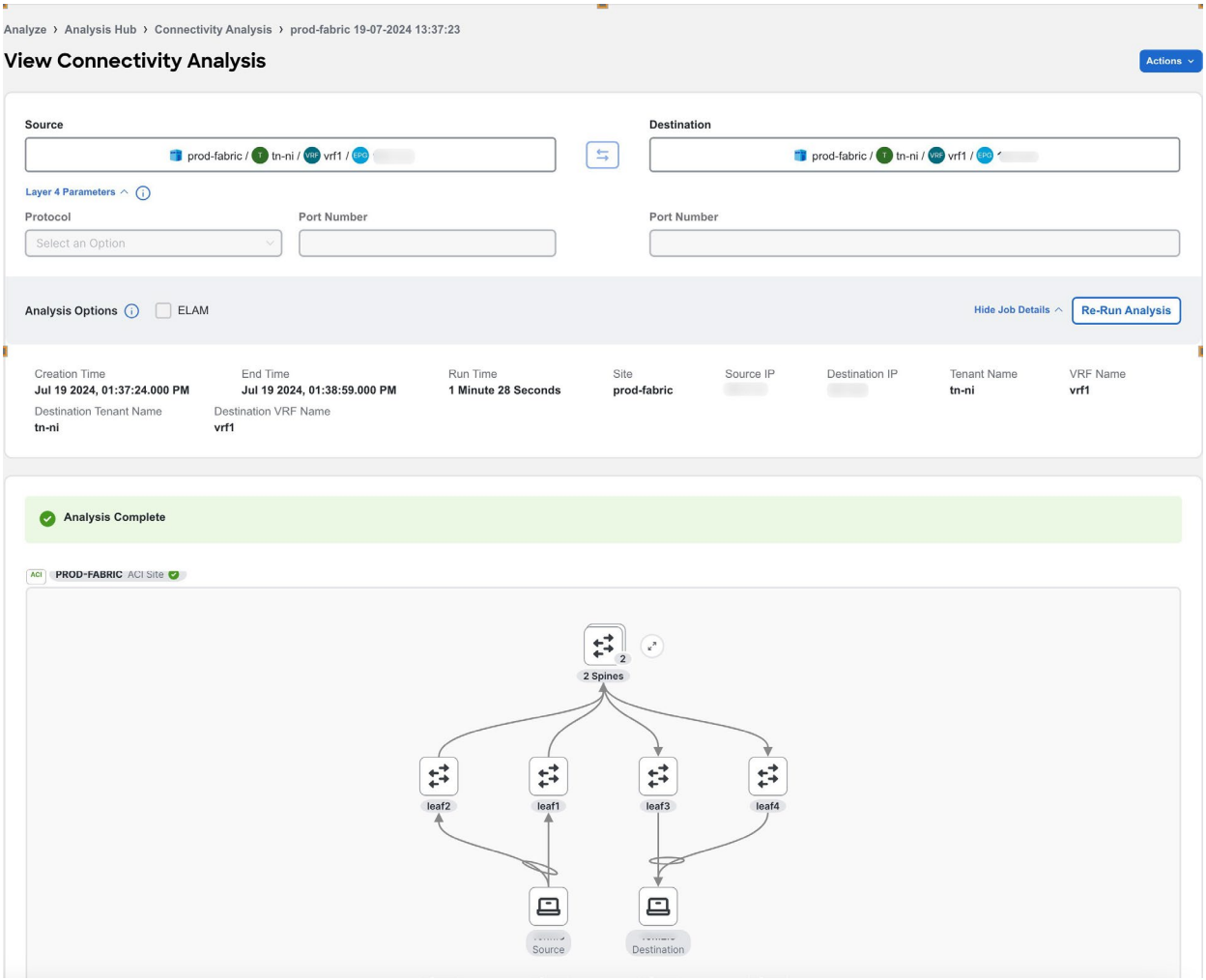
a. 分析名をクリックします。[接続分析の表示（View Connectivity Analysis）] ページで、[アクション（Actions）] ドロップダウン メニューから **[**分析の名前変更（**Rename Analysis**）**]** をクリックして名前を変更します。

接続性分析の表示

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続分析（**Connectivity Analysis**）**]** に移動します。[接続分析（Connectivity Analysis）] ジョブが表示されます。



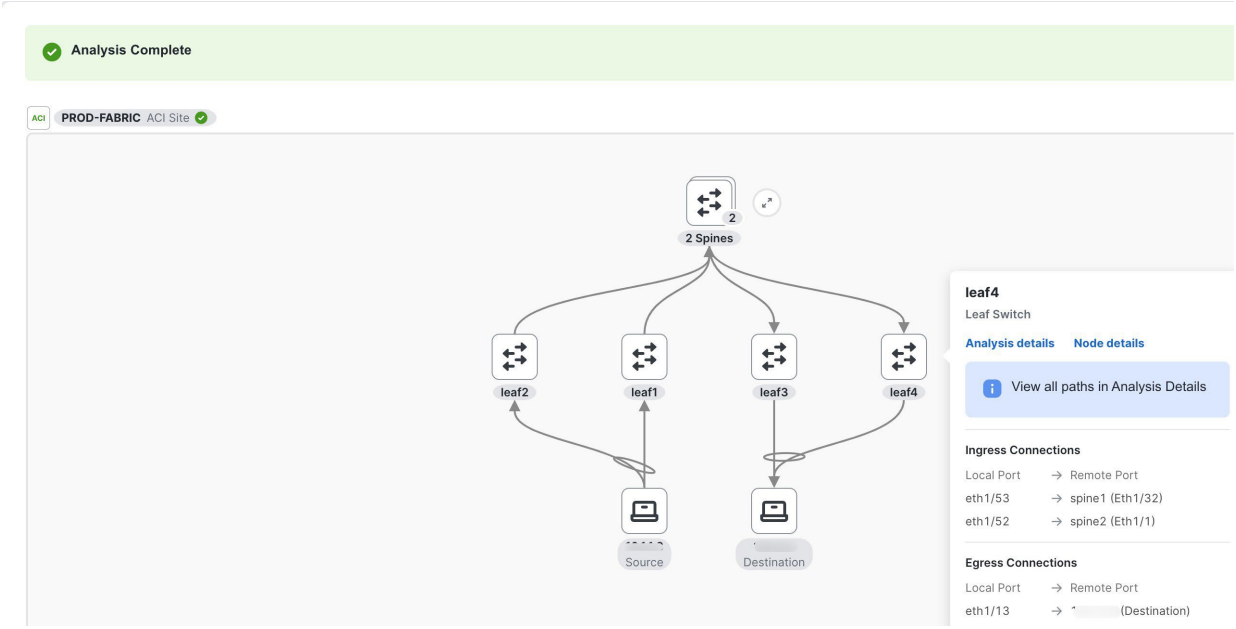
2. ドロップダウン メニューから時間範囲を選択します。
3. [概要（Summary）] エリアには、[接続分析（Connectivity Analysis）] ジョブの全体的なステータスとフロー ステータスが表示されます。
4. フィルタバーを使用して、分析をフィルタします。[接続分析（Connectivity Analysis）] テーブルには、フィルタされたジョブが表示されます。
   a. 列の見出しをクリックして、テーブルのジョブを並べ替えます。
   b. 歯車アイコンをクリックして、テーブルの列を構成します。
   c. 失敗した [フロー ステータス（Flow Status）] の上にカーソルを合わせると、詳細が表示されます。
5. **[名前（Name）]** をクリックして、接続分析の詳細を表示します。[接続分析の表示（View Connectivity Analysis）] ページでは、ジョブに入力した入力パラメータ、ジョブの詳細、トポロジを表示します。



a. [ジョブの詳細の表示（**Show Job Details**）] をクリックして、作成時間、終了時間、実行時間、ファブリック、送信元 IP、宛先 IP、送信元 VRF 名、送信元テナント名、宛先テナント名、宛先テナント名などのジョブの詳細を表示します。バナーにはジョブのステータスが表示されます。緑色のバナーは分析が成功したことを表し、赤色のバナーは分析に機能不全たことを表します。

b. [分析の再実行（**Re-run Analysis**）] をクリックして、分析を再度実行します。

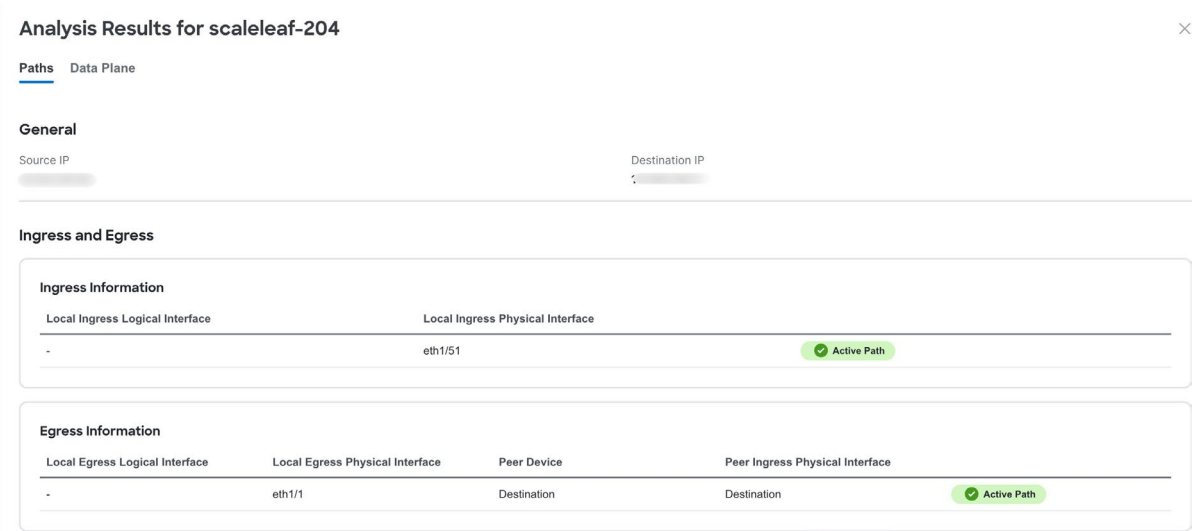
c. [トポロジ（topology）] エリアで、ファブリックの階層ビューを視覚化できます。ノードをダブルクリックして、ファブリック内のノードの相互接続を表示できます。ノード間のアクティブ パスは、緑色で強調表示されています。「トポロジ」を参照してください。



d. ノードをクリックしてツールチップを表示します。ツールチップには、ノード名、ノード タイプ、およびそのノードの入力接続と出力接続が表示されます。入力接続と出力接続では、物理インターフェイスのみが表示されます。

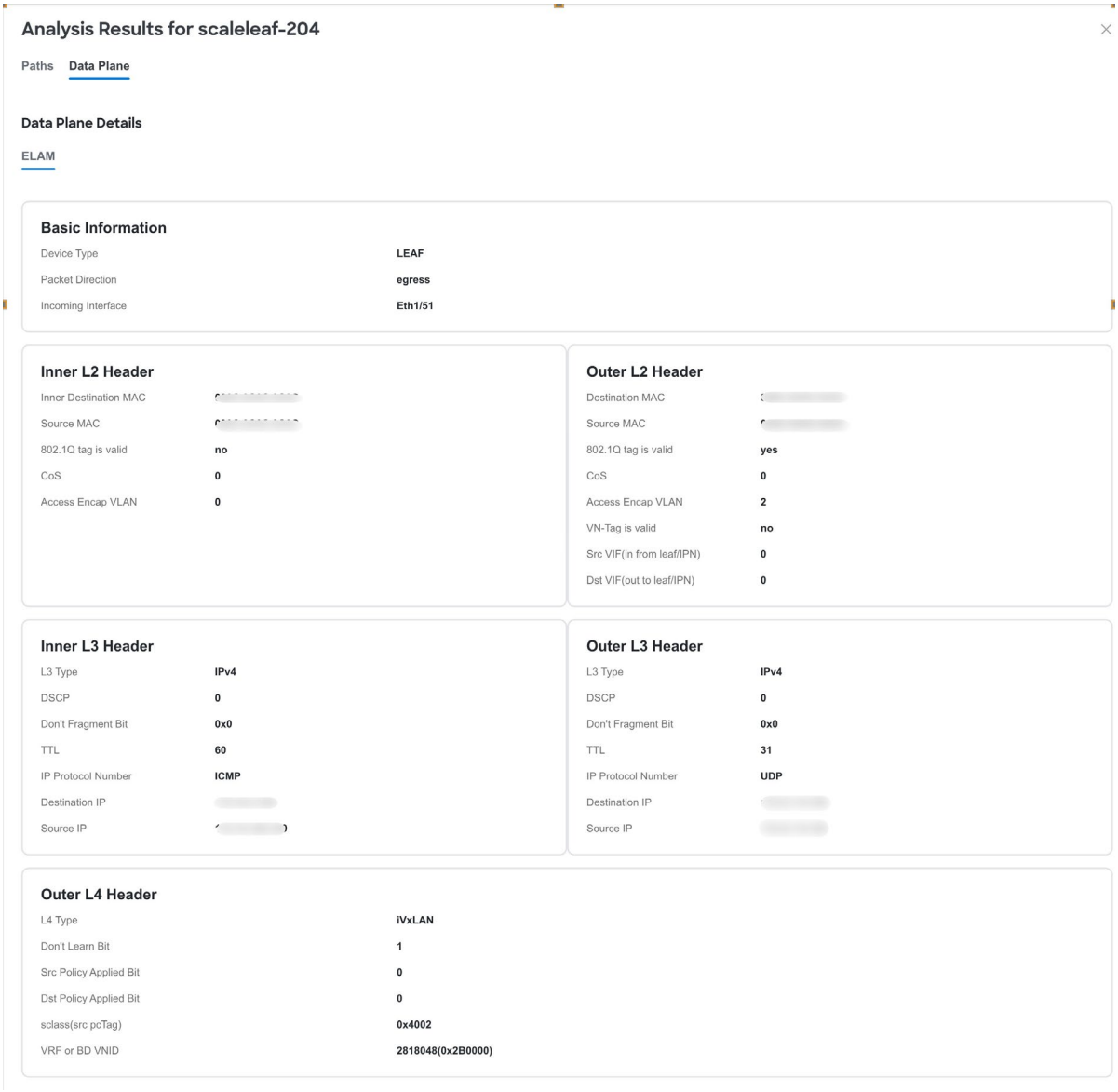
e. [分析の詳細（**Analysis Details**）] をクリックして、パスおよびデータ プレーン情報を表示します。

   i. [パス（**Paths**）] をクリックして、入力情報や出力情報などのパスの詳細を表示します。入力および出力接続エリアには、論理的なインターフェイスが表示されます。



   ii. [データ プレーン（**Data Plane**）] をクリックして、分析オプションの結果を表示します。

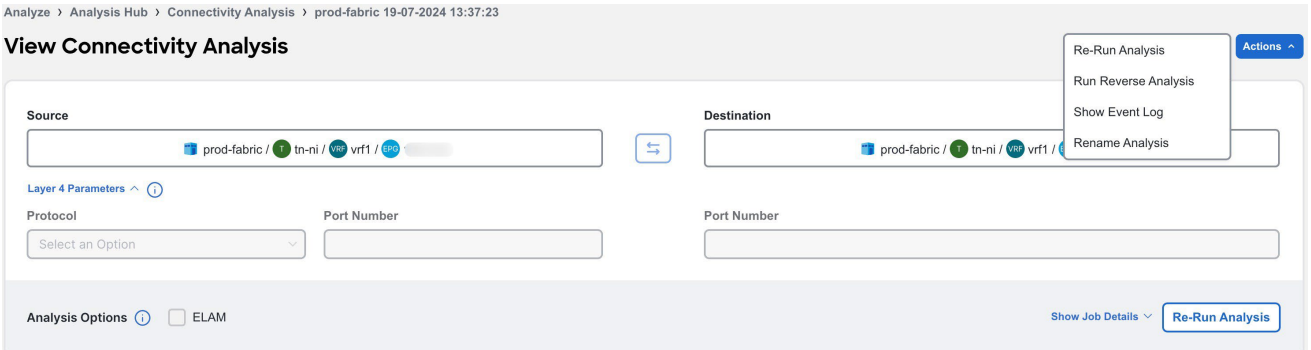
   iii. **[ELAM]** をクリックし、ELAM レポートを表示します。[フル レポートの表示（**View Full Report**）] をクリックして、レポートをダウンロードします。



f. **[**ノードの詳細（**Node Details**）**]** をクリックして、インベントリのノードの詳細を表示します。「インベントリ（Inventory）」を参照してください。

接続分析の管理

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**接続性分析（**Connectivity Analysis**）**]** に移動します。
2. **[**名前（**Name**）**]** をクリックして、接続分析の詳細を表示します。



3. [アクション（Actions）] ドロップダウン メニューから、**[**分析の再実行（**Re-Run Analysis**）**]** を選択し、分析を再度実行します。

4. [アクション（Actions）] ドロップダウン メニューから、**[**反対分析の実行（**Run Reverse Analysis**）**]** を選択し、反対方向に分析を実行します。

5. [アクション（Actions）] ドロップダウン メニューから、**[**イベント ログの表示（**Show Event Log**）**]** を選択し、分析のログを表示します。イベント ログでは、失敗した分析のエラー メッセージを確認できます。
6. [アクション（Actions）] ドロップダウン メニューから、**[**分析の名前の変更（**Rename Analysis**）**]** を選択し、分析の名前を変更します。

フィルタリング情報

一部のケースで、結果をフィルタして、より簡単に情報を見つけることができる可能性があります。

たとえば、単一のリーフ スイッチの下に多数のエンドポイントがあるが、特定の VLAN 値を持つエンドポイントにのみ関心がある場合があります。

このような場合、情報をフィルタして特定のエンドポイントのみを表示することもできます。

フィルタの絞り込みには次の演算子を使用します。

演算子	説明
==	最初のフィルタ タイプでこの演算子および後続の値を使用すると、完全一致のデータが返されます。
!=	最初のフィルタ タイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。
~ を含む	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。
!contains	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。
<	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値より小さい一致データが返されます。
< =	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値以下の一致データが返されます。
>	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値より大きい一致データが返されます。
> =	最初のフィルタ タイプ。この演算子および後続の値を使用すると、その値以上の一致データが返されます。

ログ コレクタ

ログ コレクタ

ログコレクタ機能を使用すると、ネットワーク内のデバイスのログを収集して Cisco Intersight Cloud にアップロードできます。また、Cisco TAC はファブリック上のデバイスに関するログのオンデマンド収集をトリガし、Cisco Intersight Cloud からログを取得できるようになります。

ログコレクタには次の 2 つのモードがあります。

- [ユーザー開始（User initiated）]：ユーザーはファブリック上のデバイスのログを収集し、ログ収集ジョブの完了後に収集したログを Cisco Intersight Cloud にアップロードします。ログ収集ジョブの完了後、ログファイルを Cisco Intersight Cloud に自動的にアップロードできます。
- TAC 開始 – Cisco TAC は、指定されたデバイスのログのオンデマンド収集をトリガーし、Cisco Intersight Cloud からログをプルします。

TAC 開始コレクタのデバイス接続通知機能

Nexus Dashboard Insights は、Cisco Nexus Dashboard のデバイス接続問題通知機能を使用してデバイスと通信します。通知機能は、TAC によってトリガーされたオンデマンドのログ収集をチェックします。デバイスと通信するようにファブリックが適切に構成されていない場合、Nexus Dashboard Insights から次の通知が表示されます。

- デバイスはノードの相互作用向けに設定されていません。
- デバイスでログコレクタジョブは実行できません。
- Nexus Dashboard Insights がデバイスに接続できません。

デバイスのノードの相互作用が正常でない場合、ログ コレクタがログを収集するデバイスを選択できません。GUI では、デバイスはグレー表示されています。

ログコレクタダッシュボード

[分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**ログ コレクタ（**Log Collector**）**]** に移動します。

[ログ コレクタ（**Log Collector**）**]** ダッシュボードには、特定のファブリックのジョブ ステータス別のログのグラフが表示され、最新のログ収集が表示されます。

フィルタ バーを使用すると、ステータス、名前、タイプ、ノード、開始時刻、および終了時刻

でログをフィルタ処理できます。フィルタの絞り込みには次の演算子を使用します。

演算子	説明
==	最初のフィルタ タイプでこの演算子および後続の値を使用すると、完全一致のデータが返されます。
!=	最初のフィルタ タイプ。この演算子および後続の値を使用すると、同じ値を含まないすべてのデータが返されます。

演算子	説明
~ を含む	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含むすべてのデータが返されます。
!contains	最初のフィルタタイプ。この演算子および後続の値を使用すると、その値を含まないすべてのデータが返されます。

このページには、ログ収集ジョブも表形式で表示されます。ジョブはステータスでソートされています。テーブルのログ収集ジョブを選択し、追加の詳細を表示します。

全般

これは、ジョブのステータスと、ステータス別のデバイス数を示すグラフを表示します。

詳細

次の情報が一覧表示されます。

- 作成時刻
- 終了時間（End Time）
- ノード
- Job ID

選択したノード

これにより、各ジョブのステータスおよびアップロードされたファイルのアップロードステータスとともに、ノードのリストがタブ形式で表示されます。

[すべてのファイルのアップロード（**Upload All Files**）] では、すべてのファイルをアップロードできます。

... 各ファイルを個別にダウンロードすることもできます。

TAC 開始のログコレクタ

TAC 開始のログコレクタにより、Cisco TAC は、Cisco Intersight Cloud 内の指定されたユーザーデバイスのログのオンデマンド収集をデバイスコネクタにトリガーできます。

TAC アシスト ジョブが完了すると、新しいジョブが [ログ コレクタ（**Log Collector**）] テーブルに表示されます。テーブルのログ収集ジョブを選択し、追加の詳細を表示します。**[**ログ収集（**Log Collection**）**]** ステータスには、ステータス、一般的な情報、ノードの詳細などの情報が表示されます。

ブラウザ印刷オプションがある PDF として TAC アシスト ジョブの詳細を保存できます（Chrome および Firefox でのみサポート）。

Cisco Intersight Cloud へのログのアップロード

- Nexus Dashboard Insights が Cisco Intersight Cloud に接続されていることを確認します。
- Nexus Dashboard Insights が Cisco Intersight デバイスコネクタに接続されていることを確

認します。**[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**ログ コレクタ（**Log**

Collector）**]** > **[**新しいログ コレクタ（**New Log Collector**）**]** を選択します。

1. 名前を入力します。
2. **[**ファブリックの選択（**Select Fabric**）**]** をクリックして、ファブリックを選択します。
3. （オプション）ログ収集ジョブの完了後にログ ファイルを Cisco Intersight Cloud に自動的にアップロードするには、[ログファイルの自動アップロード（Auto Upload Log Files）] をオンにします。
4. **[**次へ（**Next**）**]** をクリックします。
5. **[**ノードの追加（**Add Nodes**）**]** をクリックし、**[**ノードの選択（**Select Nodes**）**]** メニューからノードを選択します。
6. [追加（Add）] をクリックします。ノードが **[**ノードの選択（**Select Nodes**）**]** テーブルに表示されます。
7. **[**収集の開始（**Start Collection**）**]** をクリックして、ログ収集プロセスを開始します。

   ジョブが完了すると、新しいジョブが**[**ログコレクタ**]**テーブルに表示されます。

8. テーブルでジョブをクリックして、追加のジョブの詳細を表示します。
9. アイコンをクリックして、**[**ログ収集（**Log**

Collection）**]** ステータス ページを表示します。10.

   ノードを選択し、 アイコンをクリックします。

11. **[TAC** アシストにファイルをアップロード（**Upload File to TAC Assist**）**]** をクリックして、選択したノードの単一のファイルを手動でアップロードします。
12. **[**アップロード（**Upload**）**]** をクリックして、選択したノードに対して生成された

    すべてのログ ファイルを手動でアップロードします。アップロードのステータスは、

    [選択されたノード**]**テーブルに表示されます。

注意事項と制約事項

- ログのアップロードが一部のノードで失敗し、残りのノードで成功した場合、**[**選択されたノード**]** テーブルのステータスには[完了]と表示されます。
- 一部のノードの収集が失敗しても、他のノードの収集は続行されます。収集が完了すると、アップロードが開始されます。**[**選択されたノード（**Selected Nodes**）**]** テーブルでは、統合されたステータスが [ステータス（Status）] 列に表示されます。
- 一部のノードで収集が成功したが、アップロードが失敗した場合、**[**選択されたノード**]** テーブルのステータスには[失敗]と表示されます。
- **[**ログファイルの自動アップロード**]** は、一度に 1 つのノードでのみ実行できます。

トラフィック分析

トラフィック分析

トラフィック分析では、ネットワークの遅延、輻輳、ドロップをモニタできます。

トラフィック分析は、既知の TCP レイヤ 4 ポートを対応するサービス エンドポイント カテゴリと照合することで、ファブリック ネットワークで実行されているサービスを自動的に検出します。Nexus Dashboard Insights は、次のメトリックに対してしきい値に基づいてサービス パフォーマンスを評価できます。

- [遅延（Latency）]：パケットが特定のトラフィック フローの入力リーフ スイッチと出力リーフ スイッチの間を移動するのにかかる全体の時間をマイクロ秒単位で測定します。遅延は、サービス エンドポイントとそのクライアント間の入力トラフィックと出力トラフィックの両方で追跡されます。
- [輻輳（Congestion）]：ネットワーク帯域幅の使用率、Quality of Service（QoS）のアクティブ化メカニズム、プライオリティ フロー制御（PFC、および明示的輻輳通知（ECN）を測定して、サービスでネットワークの輻輳が発生しているかどうかを判断します。
- [ドロップ（Drops）]：CRC エラー、ケーブルの障害、その他のデバイスなどの要因を考慮して、ドロップされたパケットと送信されたパケットのスコアまたは数を測定します。

遅延、輻輳、ドロップなどのパフォーマンスメトリックに偏差がある場合、異常が発生します。パフォーマンス スコアは、各カンバセーションごとに計算され、サービス エンドポイントまたはエンドポイントレベルに集計され、異常を提起します。

パフォーマンス スコアは、以下に基づいて計算されます。

- 輻輳：エンドポイント間でアクティブな一貫した輻輳回避が計算されます。
- [遅延（Latency）]：前のカンバセーションの平均遅延からの偏差が計算されます。
- ドロップ：カンバセーションまたはサービスの問題に直接対応します。[ト

ラフィック分析（Traffic Analytics）] を使用すると、以下のことが可能になり

ます。

- トラフィックを広範囲にモニターできます。
- パフォーマンス メトリックに発生した異常を使用してパフォーマンスの問題を報告します。
- 上位通話サービスとクライアントをソートし、システム内の上位トーカーを特定します。
- サービスごとの SYN または RST カウントを決定します。
- オンデマンドでカンバセーションまたはフローをトラブルシューティングします。

トラフィック分析カンバセーション

TCP カンバセーションは、クライアント IP アドレス、サーバ IP アドレス、サーバ ポート、およびプロトコルを含む 4 タプルです。非 TCP カンバセーションは、送信元 IP アドレス、宛先 IP アドレス、およびプロトコルを含む 3 タプルです。単一のクライアントが、サービス エンドポイントに向けて複数の送信元ポートによって開始された複数の通信フローを確立する場合、関連するすべての統計情報がトラフィック分析テーブルの単一のエントリとして集約されます。サービスエンド ポイントは、IP アドレス、ポート、およびプロトコルによって定義されます。

カンバセーションのレート制限を超えると、異常が発生します。**[**管理者（**Admin**）**]** > **[**システム設定

（**System Settings**）] > [フロー収集（**Flow Collection**）] に移動します。[過去 1 時間のトラフィック分析ステータス（Traffic Analytics status）] 領域で、カンバセーション レートが制限に近づいているか、または超過しているかを確認できます。また、[トラフィック分析（Traffic Analytics）] のレコードがドロップしているかを

確認することもできます。

トラフィック分析のスケール制限

表には、トラフィック分析スケール制限を示します。

トラフィック分析のスケール制限

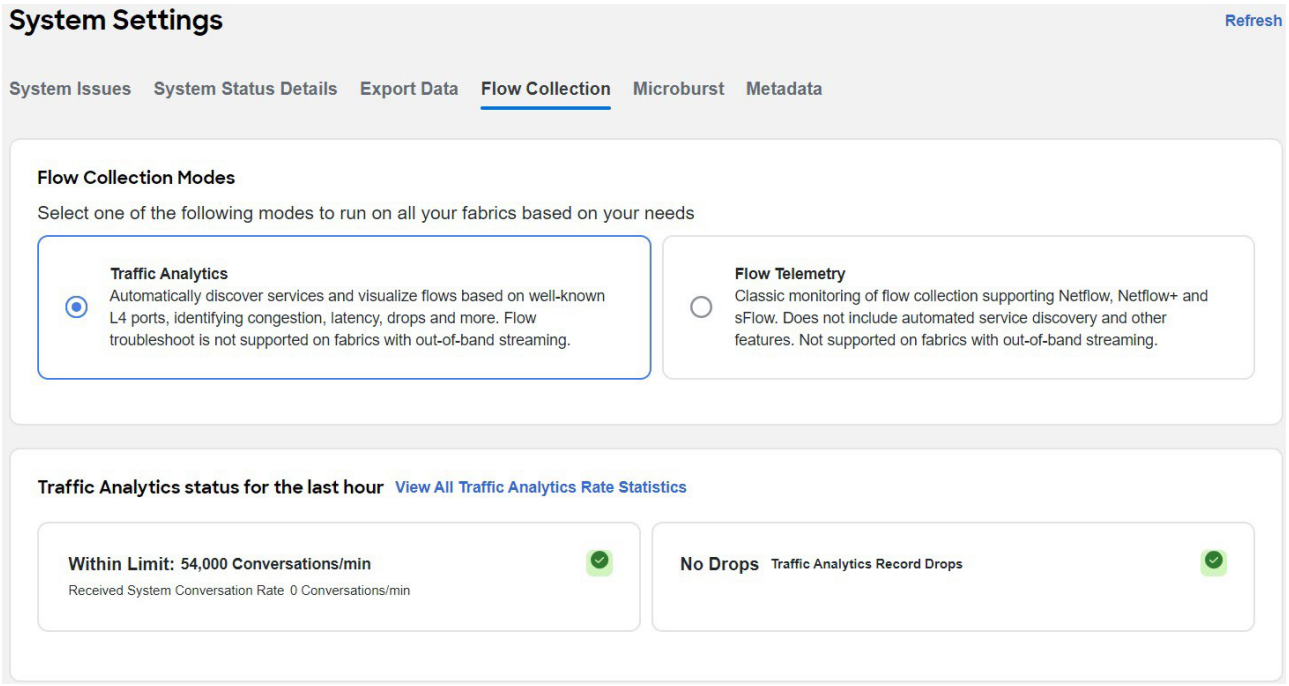
Nexus Dashboard クラスタ	**1** 分あたり固有のカンバセーション	同時進行のトラブルシューティング ジョブ
6 物理	100,000	8
3 物理	50,000	5
1 物理	5,000	1
6 仮想	10,000	5
3 リモート対応	5,000	1

トラフィック分析の注意事項および制限事項

- Nexus Dashboard Insights は、Cisco Application Policy Infrastructure Controller（APIC）リリース 6.1(1) 以降をサポートしています。
- Nexus Dashboard Insights は、リモート対応 Nexus Dashboard で 1 分あたり 5,000 件のカンバセーション、3 ノードの物理 Nexus Dashboard で 1 分あたり 50,000 件のカンバセーション、6 ノードの物理 Nexus Dashboard で 1 分あたり 100,000 件のカンバセーションをサポートします。
- [トラフィック分析（Traffic Analytics）] は Cisco ACI マルチサイトではサポートされていません。
- [トラフィック分析（Traffic Analytics）] はマルチキャストをサポートしていません。
- [トラフィック分析（Traffic Analytics）] は EX スイッチをサポートしていません。
- トラフィック分析は、ファブリック内に含まれる IPv4 または IPv6 エンドポイント間のトラフィックフローでのみ使用できます。これらのエンドポイントは、**[管理（Manage）]** > **[ファブリック（Fabrics）]** > **[接続（Connectivity）]** > **[エンドポイント（Endpoints）]** ページに表示されます。送信元または宛先エンドポイントがファブリックの外部に存在する場合、トラフィック分析移行はトラフィック分析テーブルに表示されません。
- **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[トラフィック分析（Traffic Analytics）]** に移動して、TCP サービスおよびクライアント/カンバセーションに関する情報を表示します。**[エンドポイント トラフィック分析（Endpoint Traffic Analytics）]** タブに移動して、非 TCP サービスおよびクライアント/カンバセーションに関する情報を表示します。
- Cisco APIC で NTP が設定され、PTP が有効になっていることを確認します。詳細については、『Cisco Nexus Insights 展開ガイド』 および「Precision Time Protocol (PTP) for Cisco Nexus Dashboard Insights」を参照してください。

トラフィック分析の構成

1. **[管理者（Admin）]** > **[システム設定（System Settings）]** > **[フロー収集（Flow Collection）]** に移動します。
2. **[フロー収集モード（Flow Collection Mode）]** エリアで、**[トラフィック分析（Traffic Analytics）]** を選択します。



3. **[ファブリックごとのフロー収集（Flow Collection per Fabric）]** テーブルで、ファブリックを選択します。
4. 省略記号アイコンをクリックし、**[有効化（Enable）]** をクリックしてトラフィック分析を有効にします。

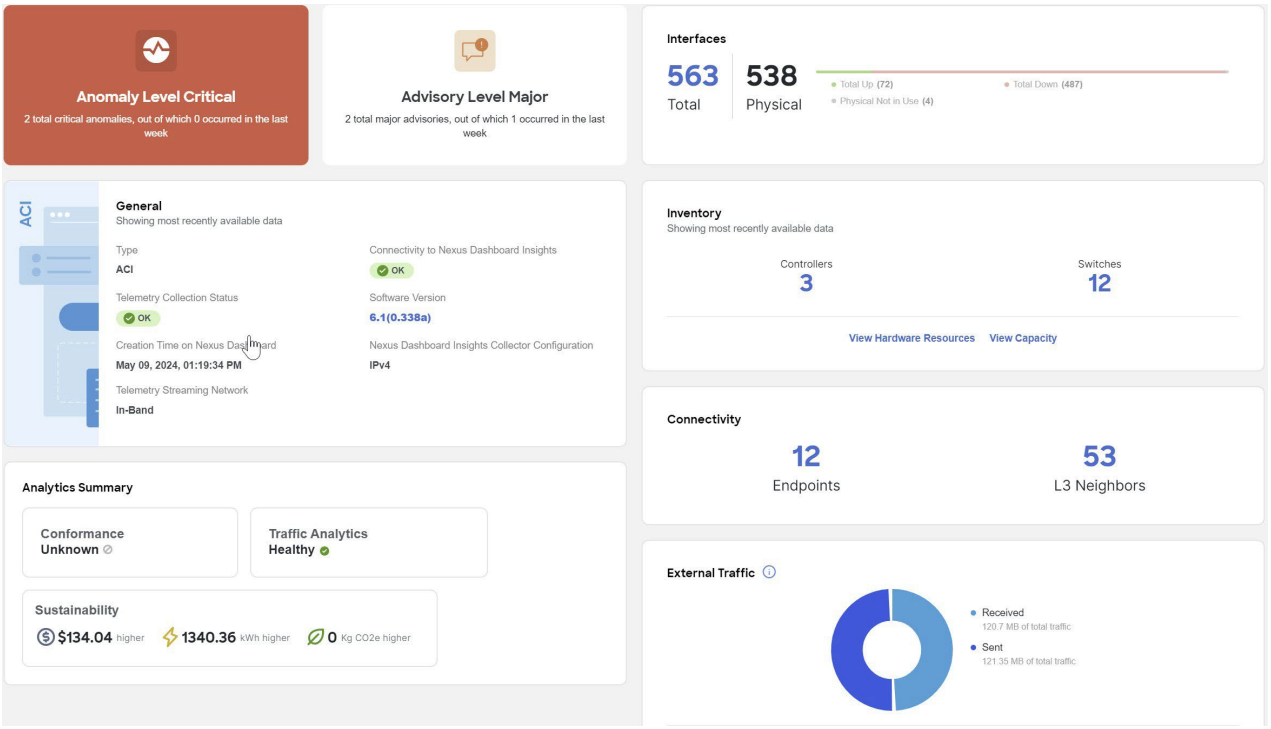
フロー テレメトリがファブリック上ですでに有効な場合、
すべてのファブリックのフロー テレメトリを最初に無効にして、[トラフィック分析 [illegible]]を有効にする前にすべてのフロー ルールを削除する必要があります。

5. [過去 1 時間のトラフィック分析ステータス（Traffic Analytics Status For The Last Hour）] 領域で、制限を超えたカンバセーションの数とトラフィック分析ドロップの数を確認できます。最大カンバセーション レート制限を超えないようにする必要があります。最大カンバセーション レート制限を超えると、フロー レコードでドロップが表示され、可視性に影響します。
6. ファブリック内の各スイッチの統計を表示するには、**[すべてのトラフィック分析レート統計の表示（View All Traffic Analytics Rate Statistics）]** をクリックします。

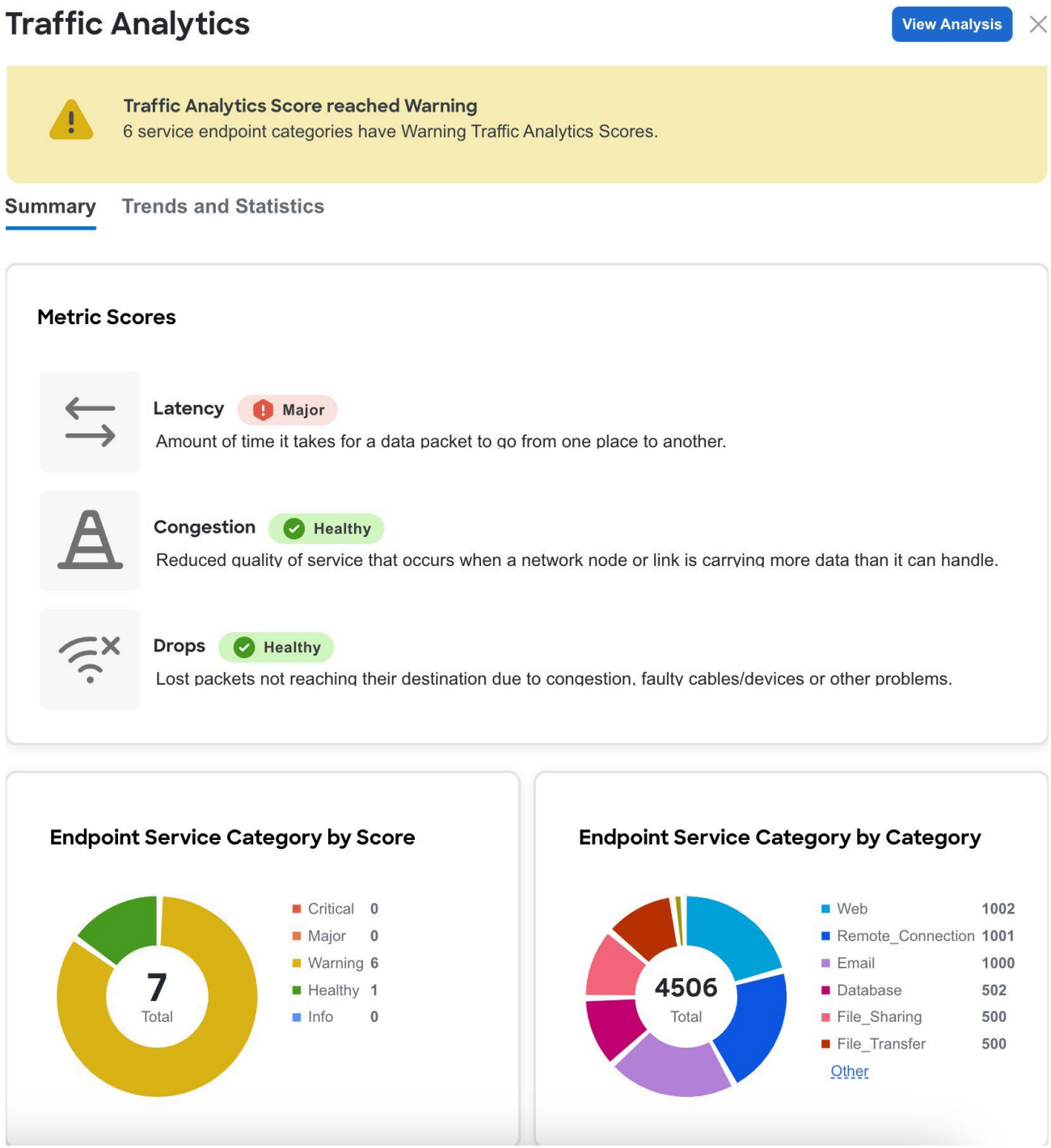
トラフィック分析の表示

個々のファブリックのトラフィック分析の表示

1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ファブリック名をクリックします。



3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (last 2 hours)）] が選択されています。
4. [分析概要（Analytics Summary）] エリアで、**[トラフィック分析（Traffic Analytics）]** をクリックして、そのファブリックのトラフィック分析の詳細を表示します。[トラフィック分析（Traffic Analytics）] ページでは、すべての情報がそのファブリックのサービス カテゴリとしてグループ化されます。



5. [概要（Summary）] 領域には、トラフィック分析スコアと、メトリックの決定方法が表示されます。エンドポイント サービス カテゴリのトラフィック プロファイルをスコアおよびカテゴリ別に表示できます。
6. **[傾向と統計（Trends and Statistics）]** をクリックして、トラフィック プロファイル、上位エンドポイント サービス スコアの変更、および上位エンドポイント カテゴリを表示します。

Traffic Analytics

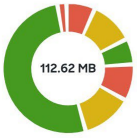
View Analysis

Traffic Analytics Score reached Warning
6 service endpoint categories have Warning Traffic Analytics Scores.

Summary | Trends and Statistics

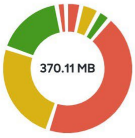
Traffic Profile

Tx



- Database 6.85 MB
- Email 11.69 MB
- File_Sharing 5.91 MB
- File_Transfer 9.36 MB
- Other

Rx



- Database 8.69 MB
- Email 11.70 MB
- File_Sharing 5.91 MB
- File_Transfer 177.97 MB
- Other

Top Endpoint Service Score Changes

Categories	Score Change	Affecting Metric
Database	Warning → Healthy	Latency ↘
File_Transfer	Warning → Healthy	Latency ↘
Remote_Connection	Warning → Healthy	Latency ↘
Email	Warning → Warning	Latency →
File_Sharing	Warning → Warning	Latency →
RoCE	Unknown → Healthy	-
Web	Warning → Warning	Latency →

7 items found

Rows per page 10 | 1

Top Endpoint Categories by Rx Latency

Categories	Average	Trend
File_Transfer	2.01 us	↗ 3%
Remote_Connection	2 us	↗ 1%
Database	2 us	↘ 0%
Email	2 us	↘ 0%
File_Sharing	2 us	→
RoCE	0 us	→
Web	2 us	↘ 0%

a. [トラフィック プロファイル（Traffic Profile）] 領域で、エンドポイント サービス カテゴリのトラフィック量を表示できます。

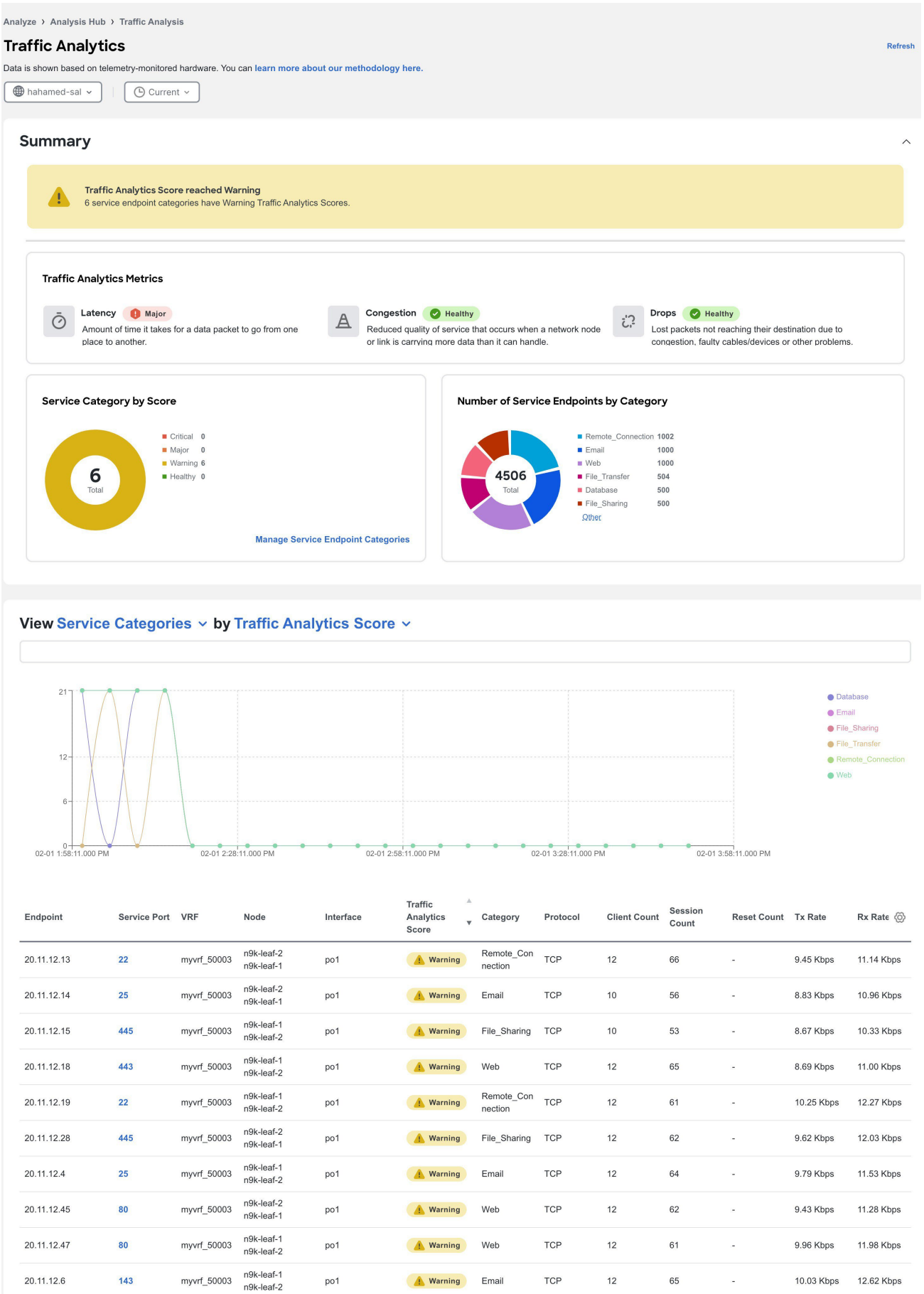
b. [上位エンドポイント サービス スコアの変化（Top Endpoint Service Score Changes）] 領域では、選択した時間範囲で異常スコアの変化と、スコアの変化に影響するメトリック（遅延、輻輳、ドロップなど）を表示できます。

c. [上位エンドポイント カテゴリ（Top Endpoint Categories by）] 領域では、Rx および Tx 遅延、輻輳スコア、およびドロップ スコア別に上位カテゴリを確認できます。

7. **[**分析の表示（**View Analysis**）**]** をクリックして、すべてのファブリックのトラフィック分析を表示します。

すべてのファブリックのトラフィック分析の表示

1. **[**分析（**Analyze**）**]** > **[**ハブの 分析（**Analyze Hub** ）**]** > **[**トラフィック分析（**Traffic Analytics**）**]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。デフォルトは **[**現在（**Current**）**]**で、過去 2 時間に確認された問題が表示されます。



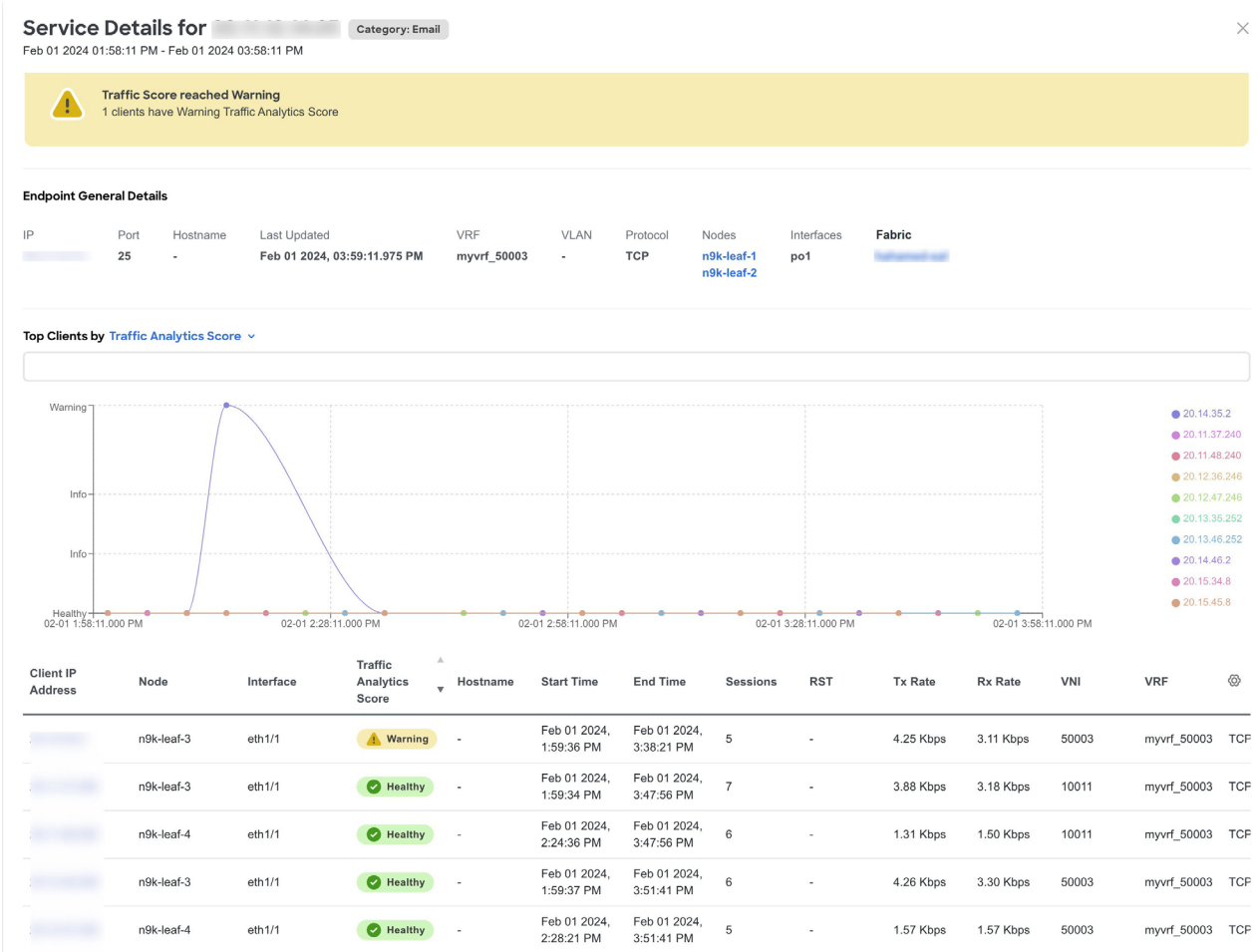
Endpoint	Service Port	VRF	Node	Interface	Traffic Analytics Score	Category	Protocol	Client Count	Session Count	Reset Count	Tx Rate	Rx Rate
20.11.12.13	22	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Remote_Connection	TCP	12	66	-	9.45 Kbps	11.14 Kbps
20.11.12.14	25	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Email	TCP	10	56	-	8.83 Kbps	10.96 Kbps
20.11.12.15	445	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	File_Sharing	TCP	10	53	-	8.67 Kbps	10.33 Kbps
20.11.12.18	443	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	65	-	8.69 Kbps	11.00 Kbps
20.11.12.19	22	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Remote_Connection	TCP	12	61	-	10.25 Kbps	12.27 Kbps
20.11.12.28	445	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	File_Sharing	TCP	12	62	-	9.62 Kbps	12.03 Kbps
20.11.12.4	25	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	64	-	9.79 Kbps	11.53 Kbps
20.11.12.45	80	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Web	TCP	12	62	-	9.43 Kbps	11.28 Kbps
20.11.12.47	80	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	61	-	9.96 Kbps	11.98 Kbps
20.11.12.6	143	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	65	-	10.03 Kbps	12.62 Kbps

4. [概要（Summary）] 領域には、トラフィック分析スコアとメトリックの決定方法が表示されます。

次に、スコアとカテゴリ別にサービス エンドポイント カテゴリの情報を表示できます。サービス エンドポイントのカテゴリでは、標準のネットワークのデフォルトと作成したカテゴリに基づいて

カテゴリに割り当てられたポートから構成されます。これらのカテゴリは動的であり、いつでも更新できます。「サービス エンドポイント カテゴリの管理」を参照してください。

5. ドロップダウン リストを使用して、トラフィック スコア、輻輳スコア、遅延スコア、ドロップ スコアなどの属性のサービス カテゴリまたはサービス エンドポイント情報をグラフ形式で表示します。[サービス エンドポイント（Service Endpoints）] を選択すると、トラフィック分析スコア、遅延スコア、輻輳スコア、ドロップ スコア、セッション数、リセット数、TX レート、Rx レートなどのさまざまな属性の上位 10 のエンドポイントも表示できます。[現在の時刻（Current Time）] で、**[トラフィック分析スコア（Traffic Analytics Score）]** の **[サービス カテゴリの表示（view Service Categories）]** を選択すると、グラフを使用して正常なスコアと異常なスコアの間の遷移を表示できます。
6. [トラフィック分析（Traffic Analytics）] テーブルでは、サービス エンドポイントの情報を表示できます。サービスまたはエンドポイントのトラフィックスコア情報は、輻輳スコア、遅延スコア、およびドロップスコアの組み合わせです。スコアが計算されると、輻輳スコアの重みが最小になり、ドロップスコアの重みが最大になります。
   a. [トラフィック分析スコア（Traffic Analytics Score）] 列にカーソルを合わせると、サービスのトラフィック分析スコアの内訳を表示できます。
   b. 検索バーを使用して、サービス カテゴリ、サービス エンドポイント値、またはその他の値でフィルタします。
   c. 歯車アイコンをクリックして、[トラフィック分析（Traffic Analytics）] テーブルの列を設定します。
7. **[サービス ポート（Service Port）]** をクリックして、特定のサービスの詳細とクライアントを表示します。



   a. [概要（Overview）] 領域では、エンドポイントの詳細と、上位クライアントやクライアントとサービス間の会話などのクライアントの詳細を表示できます。

i. [エンドポイントの一般的な詳細（Endpoint General Details）] で、[IP アドレス（IP Address）] をクリックしてエンドポイントの詳細を表示します。すべてを表示できます

そのエンドポイントでホストされているすべてのサービスと、このエンドポイントから他のサービスへの接続と IP アドレスを表示できます。

ii. ドロップダウン リストを使用して、トラフィック分析スコア別の上位クライアント、遅延スコア、ドロップ スコアなどの情報を表示します。

iii. [クライアント（Clients）] テーブルで、[トラフィック分析スコア（Traffic Analytics Score）] にカーソルを合わせると、そのクライアントのトラフィック分析スコアの内訳が表示されます。

b. [トレンドと統計（Trends and Statistics）]領域には、そのサービスのクライアント、サービス、遅延などの値のトレンドが表示されます。

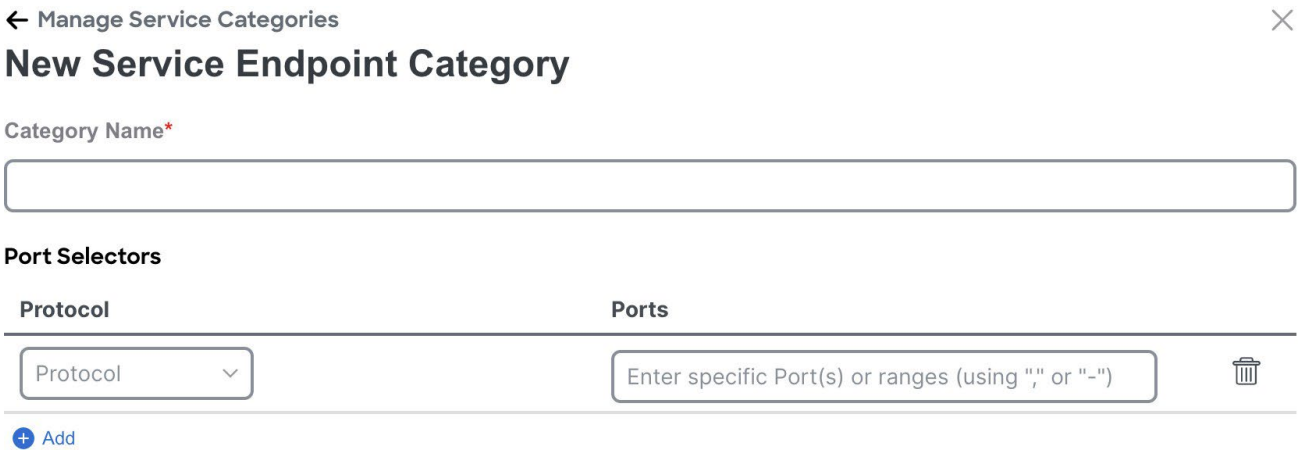
c. [異常（Anomalies）] 領域では、トラフィック スコアに基づいて特定のサービス エンドポイントの異常を表示できます。

d. [フロー収集（Flow Collections）] 領域で、そのサービスのフロー収集を表示できます。

サービス エンドポイント カテゴリの管理

[サービス エンドポイント カテゴリの管理（Manage Service Endpoint Categories）] エリアでは、標準のネットワークのデフォルトと作成したカテゴリに基づいてカテゴリに割り当てられたポートを表示できます。ポートがカテゴリに割り当てられていない場合は、既存のカテゴリのいずれかに割り当てるか、新しいカテゴリを作成できます。これにより、ネットワークポートをより効率的に整理および管理できます。

1. **[分析（Analyze）]** > **[ハブの 分析（Analyze Hub ）]** > **[トラフィック分析（Traffic Analytics）]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. [スコア別サービス カテゴリ（Service Category by Score）] エリアで、**[サービス エンドポイント カテゴリの管理（Manage Service Endpoint Categories）]** をクリックします。
4. 新しいカテゴリを作成するには、**[新しいカテゴリ（New Categories）]** をクリックします。



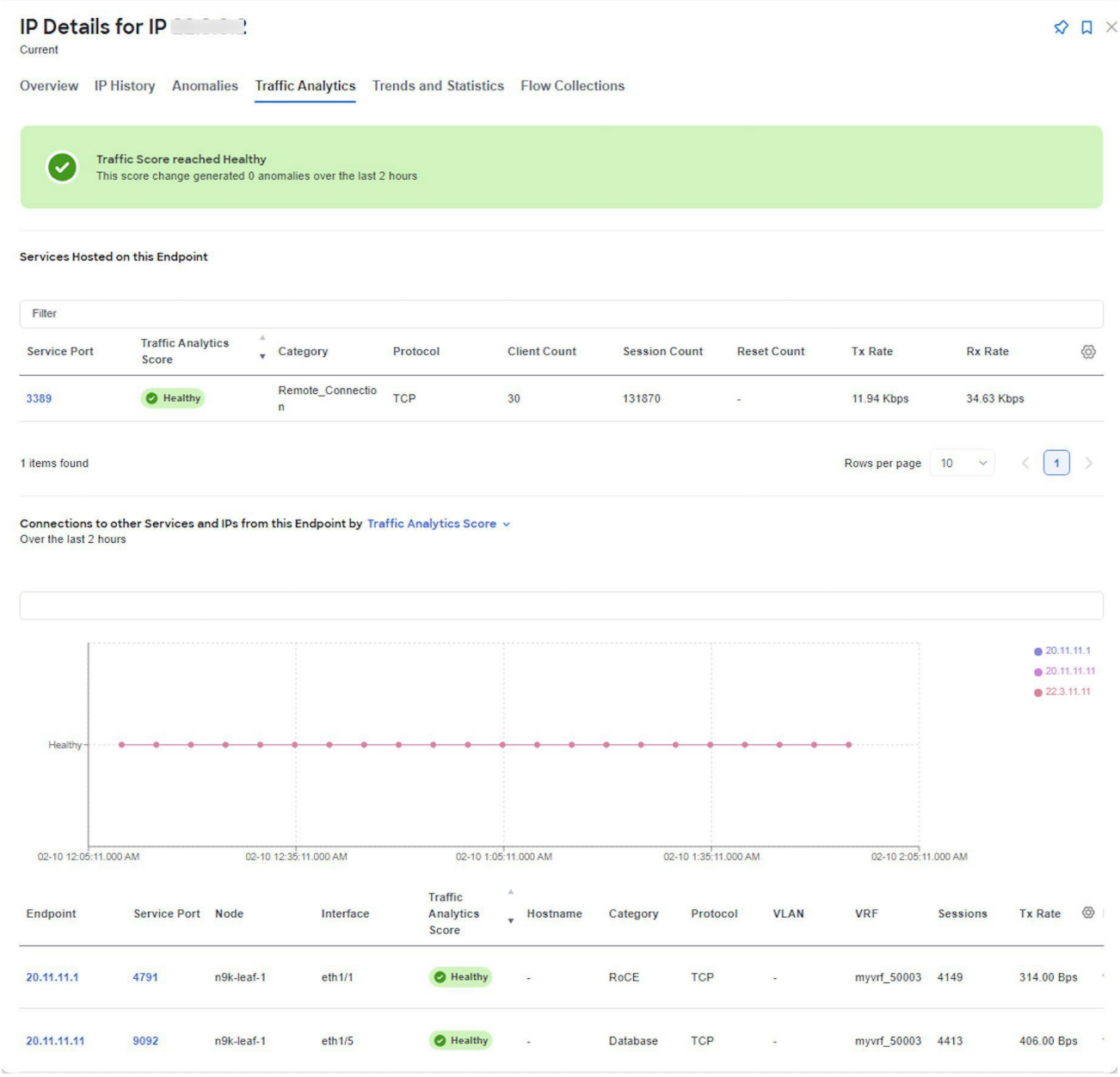
5. カテゴリの名前を入力します。
6. [プロトコル（Protocol）] ドロップダウンリストから **[TCP]** を選択します。
7. [ポート（Ports）] フィールドで、ポートまたはポート範囲を入力します。
8. **[追加（Add）]** をクリックして、プロトコルを追加します。
9. **[保存（Save）]** をクリックします。

10. カテゴリを編集するには、省略記号アイコンをクリックし、**[編集（Edit）]** を選択します。
    a. 値を編集し、**[保存（Save）]** をクリックします。

11. カテゴリを削除するには、省略記号アイコンをクリックし、**[削除（Delete）]** を選択します。
    a. **[確認（Confirm）]** をクリックします。

エンドポイントのトラフィック分析の表示

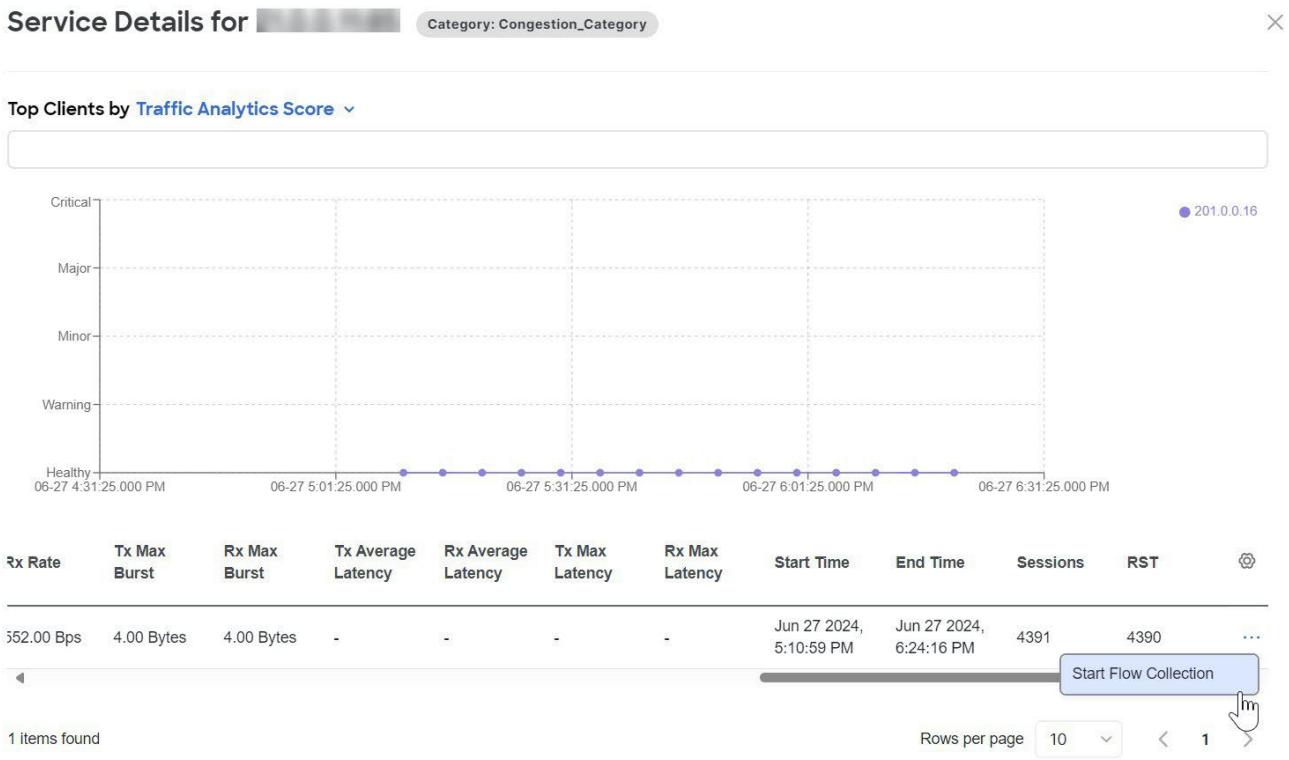
1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ファブリック名をクリックします。
3. **[接続（Connectivity）]** > **[エンドポイント（Endpoints）]** に移動します。
4. エンドポイント テーブルで、IP アドレスをクリックします。
5. [IP の詳細（IP Details）] ページで、**[トラフィック分析（Traffic Analytics ）]** をクリックして、エンドポイントのトラフィック分析ビューを表示します。



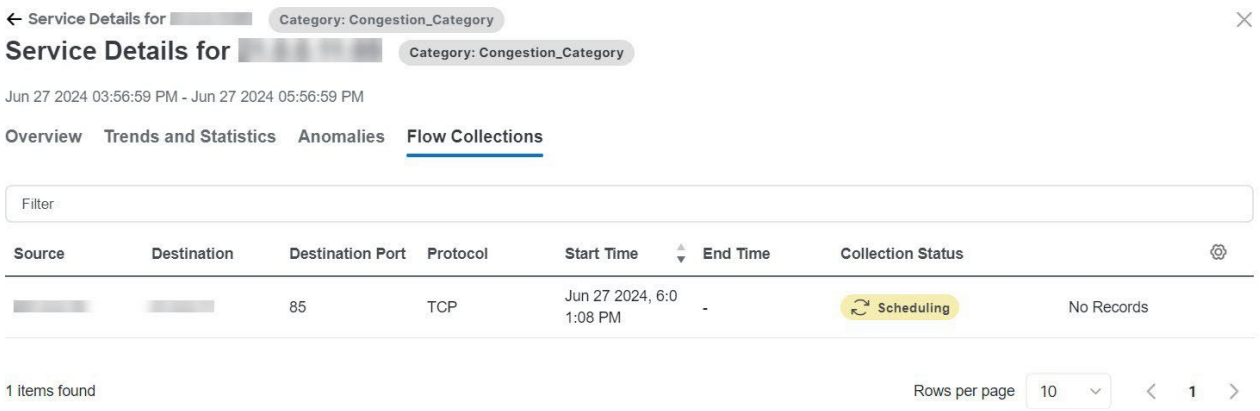
フローのトラブルシューティング ワークフロー

フロー トラブルシューティング ワークフローでは、2 つのエンドポイント間のすべてのフロー レコードを収集できます。{CiscoNIRShortName} を使用すると、フロー収集の期間を指定し、指定した期間の特定のエンドポイント間のレコードを収集できます。結果として、パスの可視化、
5 タプルのフロー情報、および個々のフローで発生した問題を表示できます。

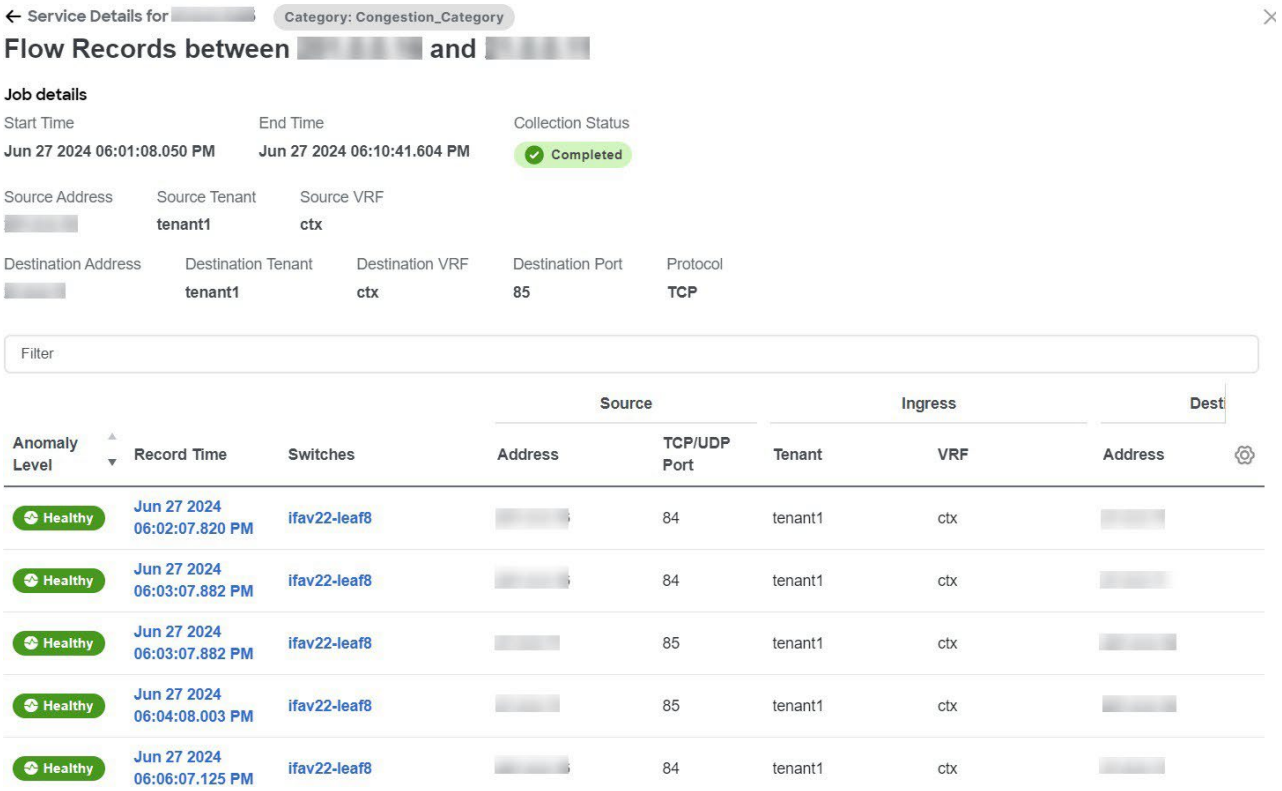
1. **[分析（Analyze）]** > **[ハブの 分析（Analyze Hub ）]** > **[トラフィック分析（Traffic Analytics）]** の順に選択します。
2. ドロップダウン メニューからファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。デフォルトでは、[現在の時刻（過去 2 時間）（Current time (last 2 hours)）] が選択されています。
4. **[ビュー別（View by）]** エリアのテーブルで、エンドポイントを選択し、[サービス ポート（Service Port）] にあるエンドポイントのポート番号を
クリックします。
5. [サービスの詳細（Service Details）] ページで、クライアント IP アドレスの省略記号アイコンをクリックし、**[フロー収集の開始（Start Flow Collection）]** を選択します。省略記号アイコンを確認するには、クライアント IP アドレスのテーブルを右までスクロールする必要がある可能性があります。



6. 特定の期間のフロー レコードのサンプルを収集する期間を選択します。**[開始してフロー収集タブに移動する（Start and go to Flow Collections Tab）]** をクリックします。



7. [収集ステータス（Collection Status）] に [完了（Completed）] と表示されたら、**[**レコードの表示（**View Records**）**]** をクリックして、その特定のサービス エンドポイントのフロー レコードの詳細を表示します。



8. ファブリックのフロー収集を表示するには、**[管理（Manage）]** > **[ファブリック（Fabrics）]** の順に選択し、ファブリックを選択して、
[接続（Connectivity）] > **[フロー収集（Flow Collections）]** をクリックします。
9. 非 TCP フローのフロー収集を実行するには、次のサブステップを実行します。
   a. エンドポイント テーブルで、エンドポイントポイントのサービスポートをクリックします。そのエンドポイントの **[サービスの詳細（Service Details）]** ページが表示されます。
   b. **[エンドポイントの全般の詳細（Endpoint General Details）]** エリアで、IP アドレスをクリックします。その IP アドレスの **[IP アドレス（IP Details）]** ページが表示されます。
   c. **[トラフィック分析（Traffic Analytics）]** タブをクリックします。
   d. エンドポイント テーブルで、エンドポイントの省略記号アイコンをクリックし、**[フロー収集の開始（Start Flow Collection）]** を選択します。省略記号アイコンを表示するには、エンドポイントのテーブルを右端までスクロールする必要がある場合があります。

フローのトラブルシューティングでは、次のシナリオでは、各レコード のパケットが通過するすべてのスイッチが表示されない場合があります。

- Nexus Dashboard Insights にフロードロップがある場合
- ハードウェアでテーブルの衝突が発生した場合

持続可能性レポート

持続可能性レポート

Nexus Dashboard Insights サステナビリティ レポートは、ネットワークのエネルギー使用量、関連する炭素排出量、総エネルギー コストをモニタリング、予測、改善するために役立ちます。サステナビリティ レポートでは、すべてのファブリックのエネルギー使用量、CO2 排出量、エネルギー コストに関するインサイトを月単位で取得できます。

レポートは、消費電力の月次値を計算し、選択した月の 1 日ごとに、各ファブリックのすべてのデバイスの使用量データを合計することで作成されます。このデータを Cisco Energy Manager と組み合わせることで、エネルギー コスト、推定排出量、推定スイッチ消費電力の観点で、その使用状況が何を意味するのかをより深く理解することができます。Cisco Energy Manager に関する詳細は、「Cisco Energy Manager」を参照してください。

レポートの概要エリアには、総低コスト、想定スイッチ電力消費、排出源、推定排出量などの情報を含んでいます。

- 推定コストでは、毎月のエネルギー使用量に基づいて、ファブリックの電気料金の予想される増減を把握できます。
- 予想されるスイッチ消費電力を使用すると、スイッチが電力をどの程度効率的に使用しているかを把握できます。[予想される PDU 電力消費量（Estimated PDU Power Consumption）] により、デバイスまたは Panduit 配電ユニット（PDU）が使用している電力量の詳細を示します。
- 推定 CO2 排出量では、使用する電力源と量に基づいて、ファブリックによる持続可能性への取り組みが総 CO2 排出量に及ぼす影響を把握できます。

Nexus Dashboard に Panduit PDU をオンボードしている場合、you can use the **[データ ソース（Data Source）]** トグルを使用して、サステナビリティ レポートで 2 つの異なる電気数値を確認できます。1 つはスイッチのみ、1 つは PDU です。

- [スイッチ データ（Switch Data）]：ファブリックに追加された個々のスイッチによって報告された電力データのみを使用
- [PDU データ（PDU Data）]：サポートされている PDU によって報告された電力データを使用します。このデータには、スイッチ、ファン、および PDU に物理的に接続されているその他のデバイスが含まれます。

[データソース（Data Source）] トグルで選択した値に応じて、推定コストや CO2 排出量など、他のメトリックに対して計算される値が変わります。

サステナビリティを活用して、以下のことが可能です。

- ファブリックのエネルギー料金の上昇をさらに予測し、予算が実際の使用量をより正確に反映するようにします。
- 個々のファブリックの 1 時間ごとのエネルギー使用量をより追跡します。使用料を分散させてピーク時間帯の割増料金を避けることで、長期的に電気代を下げることができる可能性があります。
- ファブリックを実行している際に気候変動に与える直接的なサステナビリティへの影響を確認します。経時的に CO2 排出量を追跡することで、低炭素排出源を選択し、ESG 目標の達成に向けた進捗状況を追跡することも促進されます。

Nexus Dashboard Insights のサステナビリティ レポートの保持時間は 12 か月間です。

Cisco Energy Manager

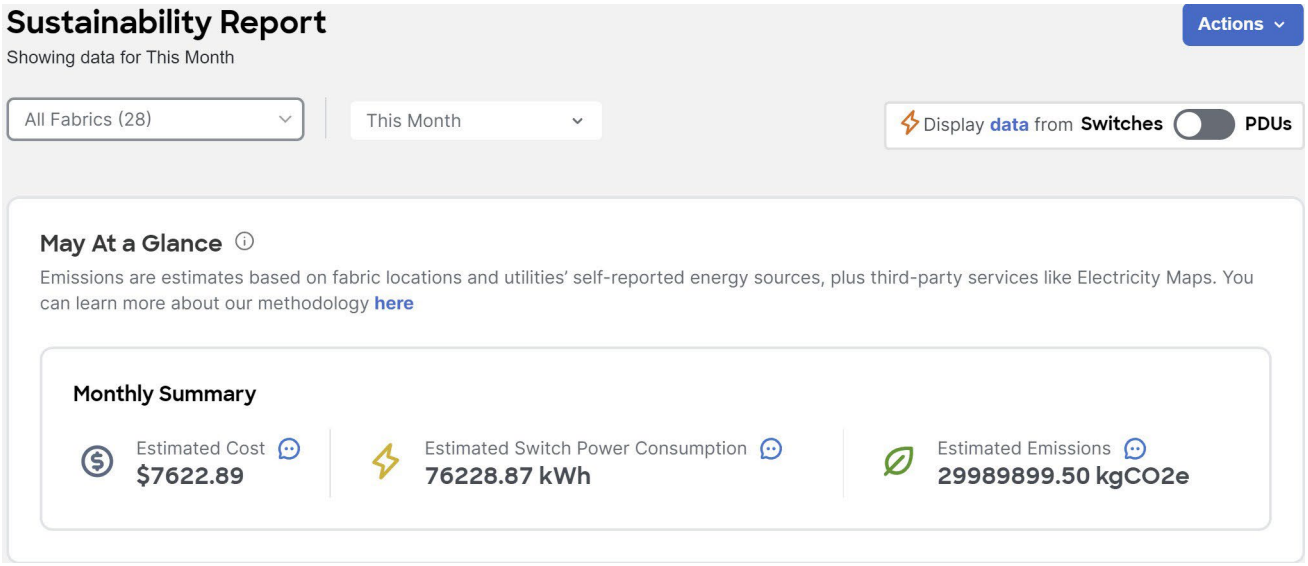
Cisco Energy Manager は Cisco により開発されたサービスであり、さまざまなデータ プロバイダからデータを収集し、データから GHG 排出量とエネルギー源を統合します。Cisco Energy Manager は、Cisco Intersight クラウドでホストされます。

スイッチのサステナビリティ レポートの表示

1. **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[サステナビリティ レポート（Sustainability Report）]** に移動します。
2. ドロップダウン メニューから、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。
4. **[次のデータを表示（Display data from）**] トグルを活用して、スイッチからのデータを表示します。
5. **[レポートの準備（Prepare Report）]** をクリックします。

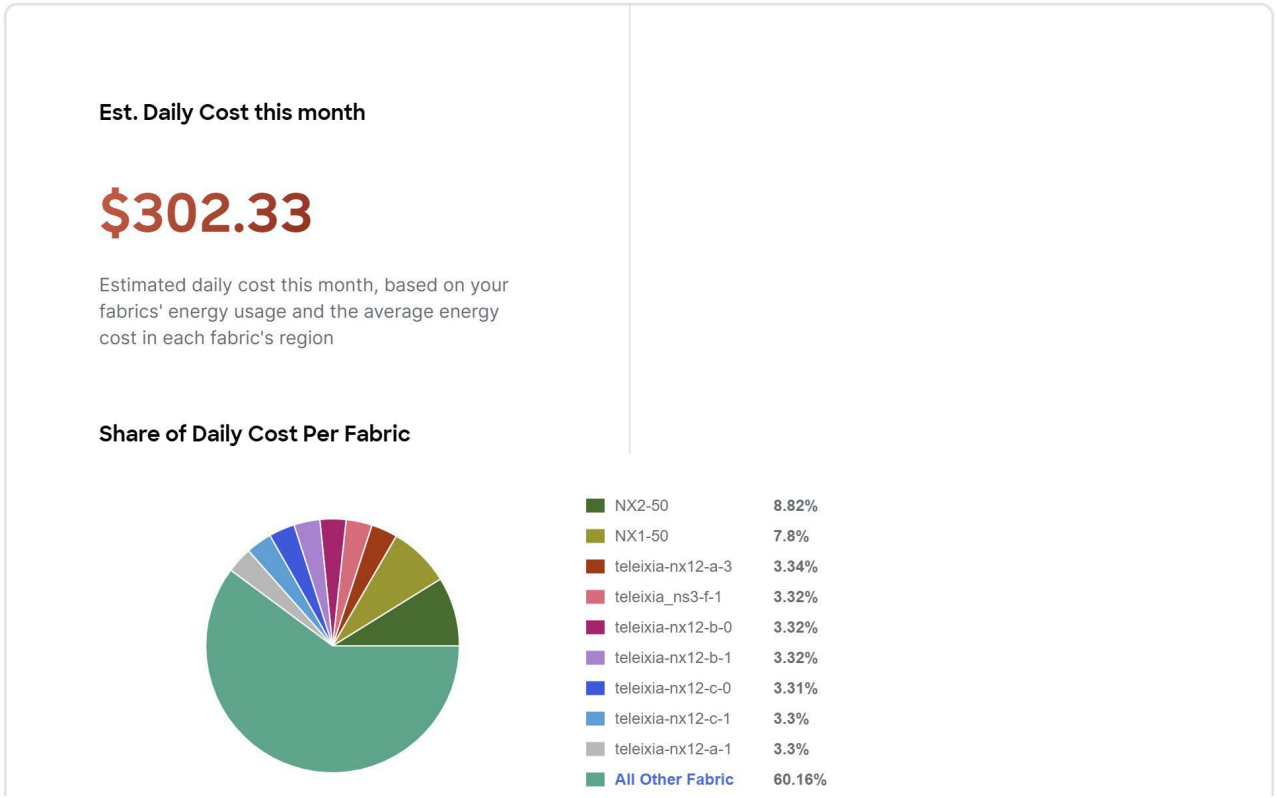
   サステナビリティ レポートには、選択した月の特定のファブリックの概要、コスト、エネルギー、および排出量の情報が表示されます。

6. **[概要（At A Glance）]** エリアを調べて、選択した月の推定コスト、推定スイッチ電力消費量、および推定排出量の概要を確認します。**[詳細（Learn More）]** アイコンをクリックします。

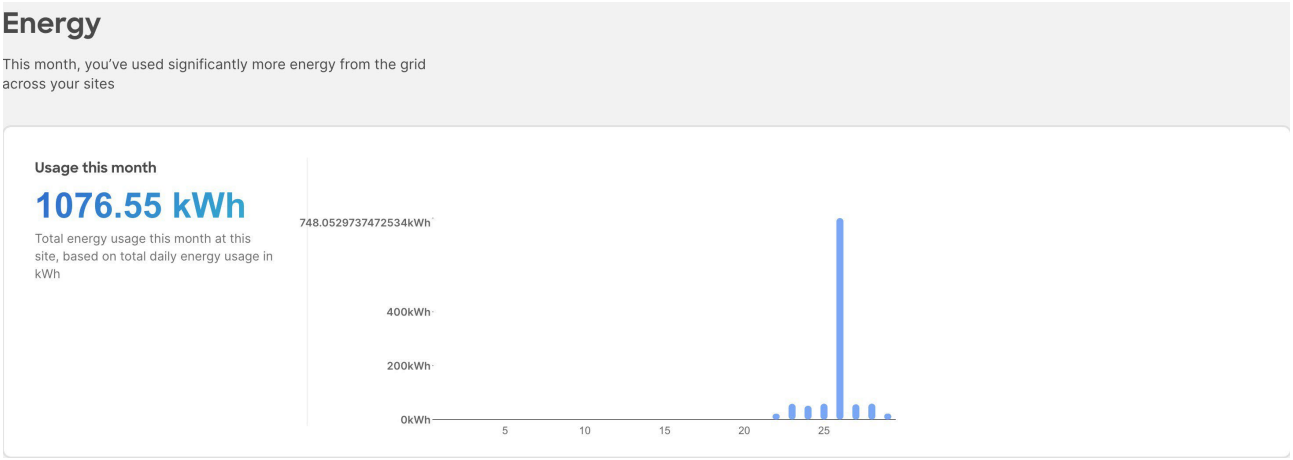


7. **[コスト（Cost）]** エリアを確認し、選択した月の 1 日あたりの推定コストと、ファブリックごとの 1 日あたりのコスト共有を確認します。

Cost

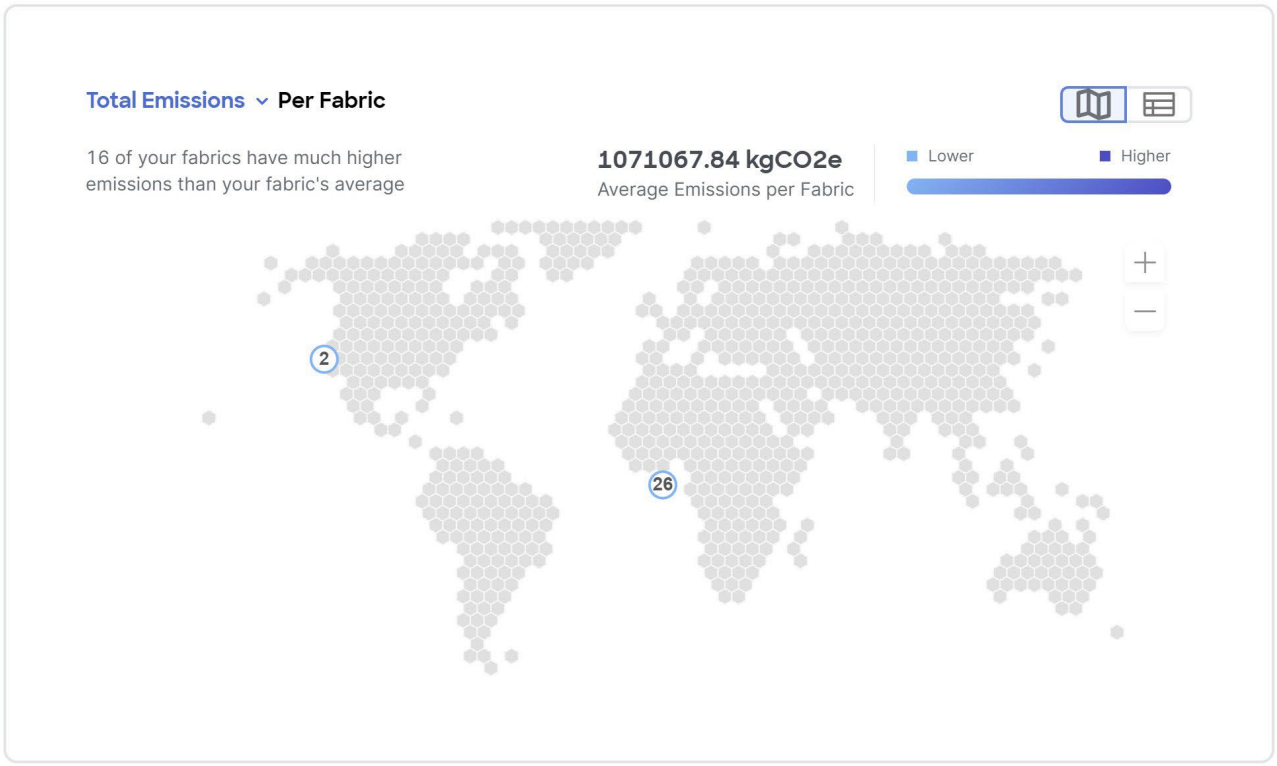


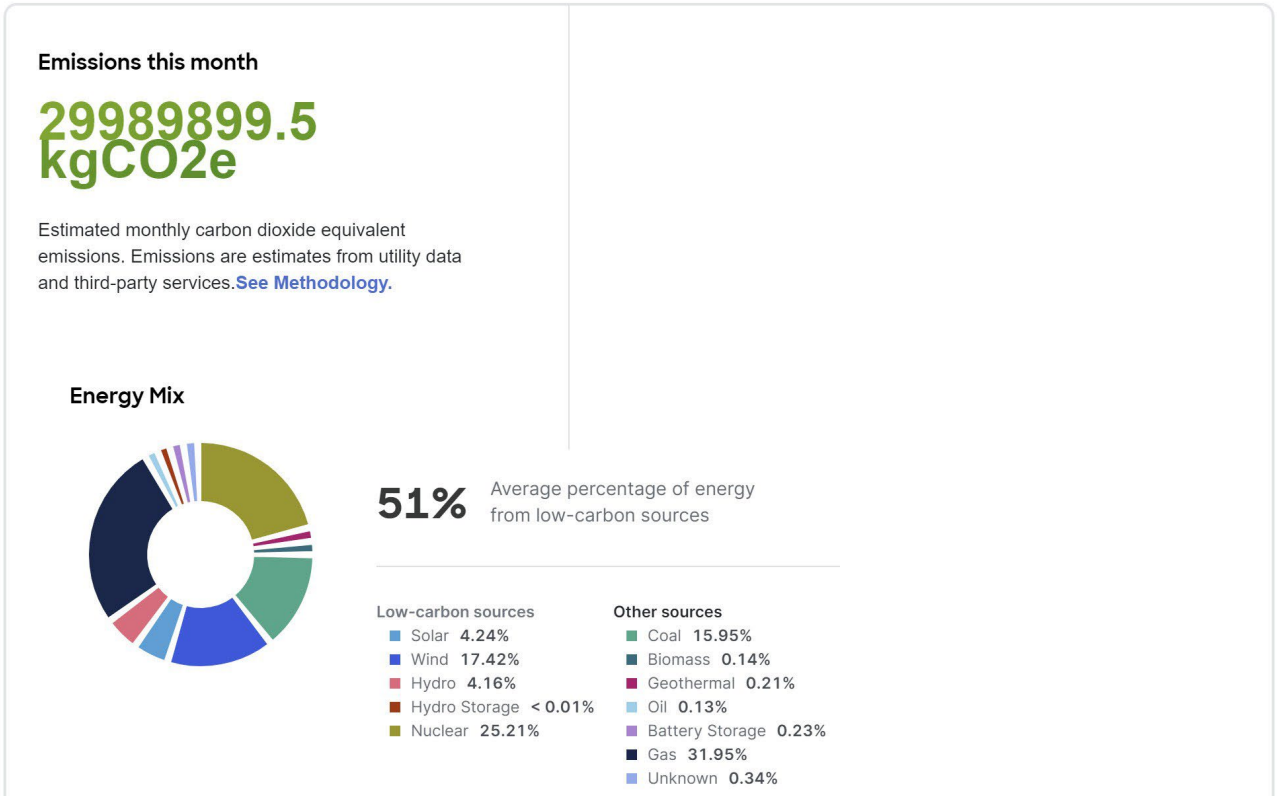
8. （オプション）[アクション（ **Actions** ）] メニューから [ファブリックエネルギー設定（ **Fabric Energy** 設定 ）] を選択し、より正確な見積書を得るために当月の平均コストをカスタマイズします。推定コストを算出するには、Nexus Dashboard Insights は、各リージョンのグリッド エネルギーの平均コストに基づく値を使用しています。
9. **[**エネルギー（ **Energy**） **]** エリアを調べて、選択した月のエネルギー使用量を kWh 単位で確認します。



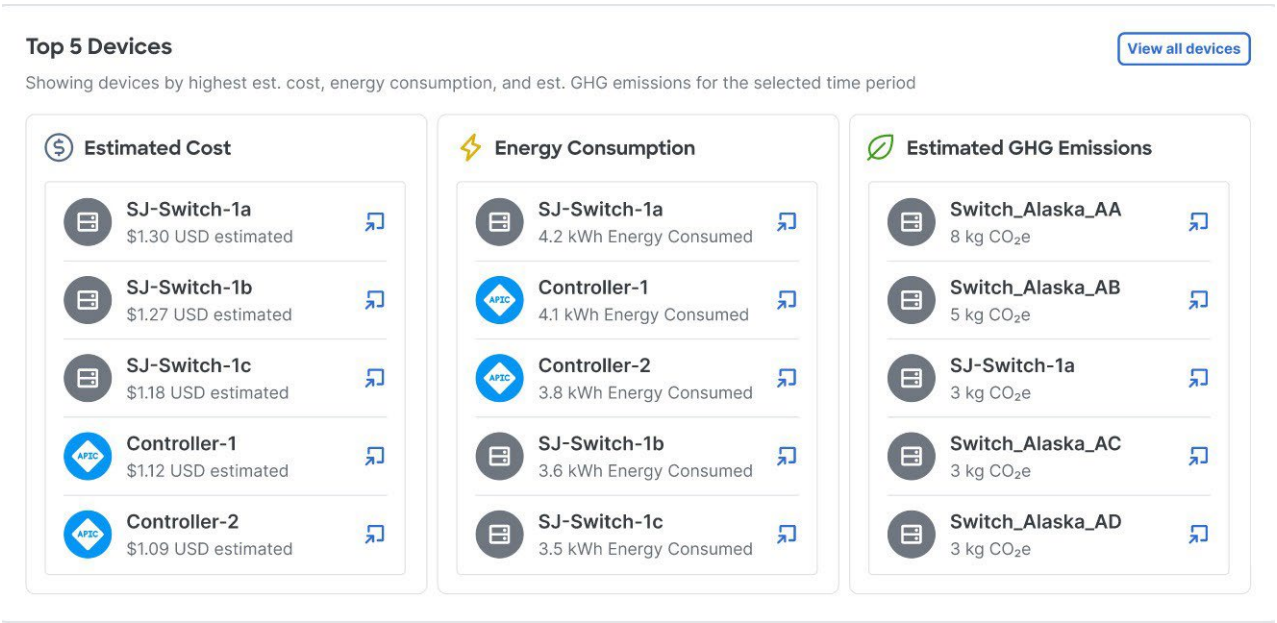
10. **[**排出量（**Emissions**）**]** エリアでは、ファブリックごとの総排出量または効率指標、月ごとの推定される二酸化炭素換算排出量、低炭素エネルギー源およびその他のエネルギー源からのエネルギーの平均割合、選択した月のすべての日で各 3 時間のレポート期間中に使用されたエネルギー源の総排出量の割合を確認することができます。

    ファブリックごとの総排出量または効率指標については、トグルを使用してグラフ形式または表形式で情報を表示します。





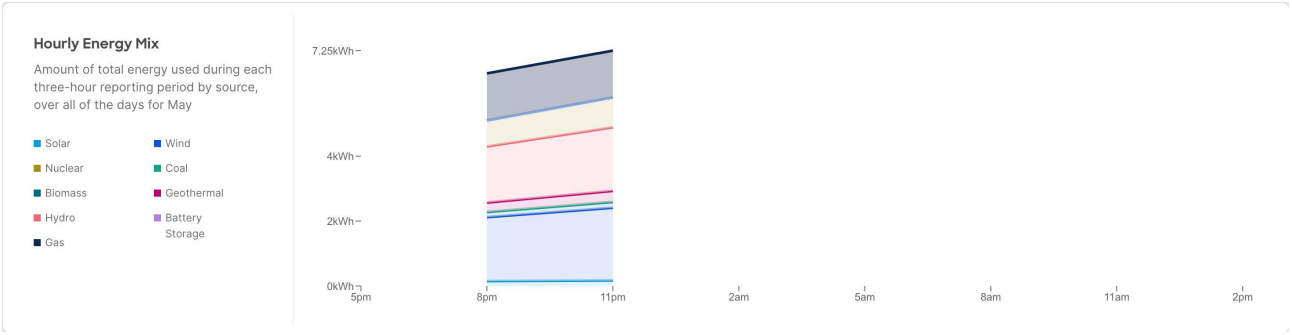
11. **[上位 5 デバイス（Top 5 Devices）]** エリアを調べて、推定コスト、消費電力量、および推定温室効果ガス（GHG）排出量が最も高い上位 5 つのデバイスを確認します。



[すべてのデバイスの表示（**View all devices**）**]** をクリックし、上位 5 デバイスだけではなく、すべてのデバイスのデータを確認します。

12. [ファブリック（fabric）] ドロップダウン メ ニューからファブリックを選択して、1 時間あたりのエネルギー混合を表示します。

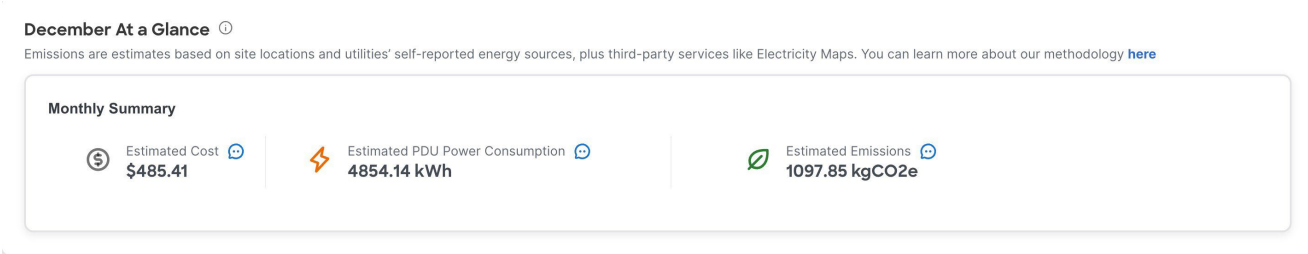
    時間ごとのエネルギー効率は、選択した月のすべての日で各 3 時間のレポート期間中に使用された総エネルギー量をソース別に表示します。次のレポートを生成できるようになるまでの最小期間は 3 時間です。



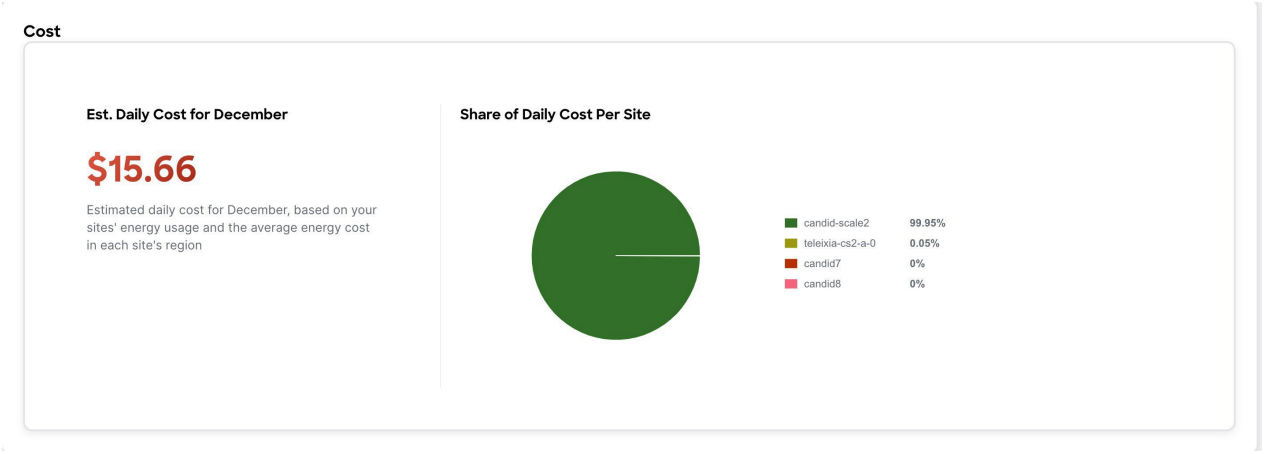
PDU のサステナビリティ レポートの表示

1. **[**分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**サステナビリティ レポート（**Sustainability Report**）**]** に移動します。
2. ドロップダウン メニューから、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
3. ドロップダウン メニューから時間範囲を選択します。
4. **[**次のデータを表示（**Display data from**） **]** トグルを活用して、PDU からのデータをディスプレイします。
5. **[**レポートの準備（**Prepare Report**）**]** をクリックします。

   サステナビリティレポートには、選択した月の特定のファブリックの概要、コスト、エネルギー、および排出量の情報が表示されます。
6. **[概要（At A Glance）]** エリアを調べて、選択した月の推定コスト、推定スイッチ電力消費量、および推定排出量の概要を確認します。**[詳細（Learn More）]** アイコンをクリックします。



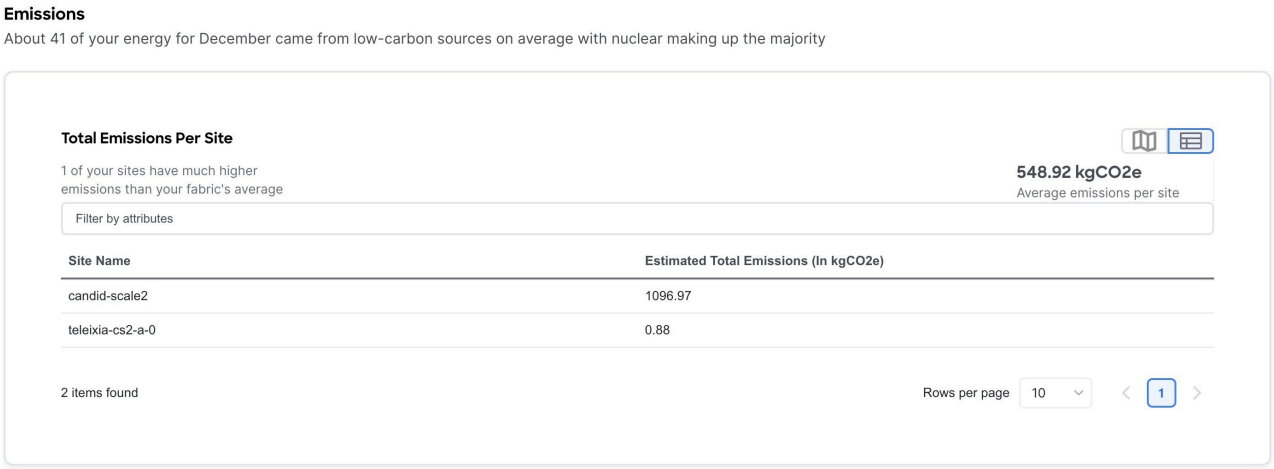
7. **[**コスト（**Cost**）**]** エリアを確認し、選択した月の 1 日あたりの推定コストと、ファブリックごとの 1 日あたりのコスト共有を確認します。



8. （オプション）[アクション（ **Actions** ）] メニューから [ファブリックエネルギー設定（ **Fabric Energy** 設定 ）] を選択し、より正確な見積書を得るために当月の平均コストをカスタマイズします。推定コストを算出するには、Nexus Dashboard Insights は、各リージョンのグリッド エネルギーの平均コストに基づく値を使用しています。
9. **[**エネルギー（ **Energy**） **]** エリアを調べて、選択した月のエネルギー使用量を kWh 単位で確認します。

10. **[**排出量（**Emissions**）**]** エリアでは、ファブリックごとの総排出量、月ごとの推定される二酸化炭素換算排出量、低炭素エネルギー源およびその他のエネルギー源からのエネルギーの平均割合、選択した月のすべての日で各 3 時間のレポート期間中に使用されたエネルギー源の総排出量の割合を確認することができます。

    ファブリックごとの総排出量については、トグルを使用して、グラフ形式または表形式で情報を表示します。

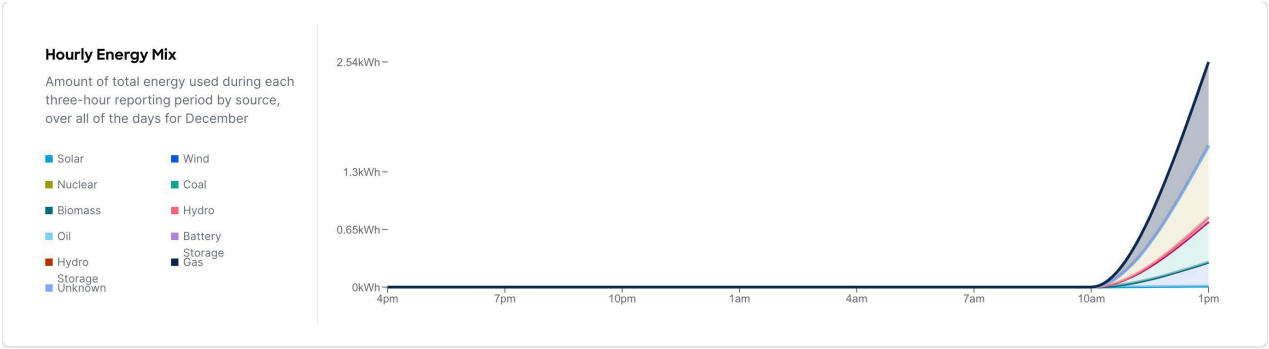


11. **[上位 5 デバイス（Top 5 Devices）]** エリアを調べて、推定コスト、消費電力量、および推定温室効果ガス（GHG）排出量が最も高い上位 5 つのデバイスを確認します。

    [すべてのデバイスの表示（View all devices）] をクリックし、上位 5 デバイスだけではなく、すべてのデバイスのデータを確認します。

12. [ファブリック（fabric）] ドロップダウン メ ニューからファブリックを選択して、1 時間あたりのエネルギー混合を表示します。

    時間ごとのエネルギー効率は、選択した月のすべての日で各 3 時間のレポート期間中に使用された総エネルギー量をソース別に表示します。次のレポートを生成できるようになるまでの最小期間は 3 時間です。



デルタ分析

デルタ分析

Nexus Dashboard Insights は定期的にサイトの分析を実行し、データはノード数に応じた間隔で収集されます。

ノード数	**Interval**
100 人未満	2 時間
100 ～ 400	3 時間
400 以上	12 時間

Nexus Dashboard Insights は、各間隔でコントローラポリシーとファブリックに関する実行時の状態のスナップショットをキャプチャし、分析を実行して、異常を生成します。生成された異常は、スナップショット時点でのネットワークの状態を表します。

差分分析を使用すると、2 つのスナップショット間のポリシー、実行時の状態、およびネットワークの状態の違いを分析できます。

[差分分析の作成（**Create Delta Analysis**）**]**：新しい差分分析を作成し、既存の分析を管理できます。「差分分析の作成」を参照してください。

正常性の差分

正常性の差分では、2 つのスナップショット間におけるファブリックの正常性の違いを分析しま

す。詳細については、 「正常性差分分析の表示」 を参照してください。

ACI のポリシーの差分

ポリシーの差分では、2 つのスナップショット間のポリシーの違いを分析し、ACI ファブリックの変更点の相互に関連するビューを提供します。

詳細については、 「ポリシー差分分析のビュー」 を参照してください。

差分分析の注意事項と制約事項

- 現在、一度に複数の差分分析を作成できますが、一度に複数の差分分析をキューに入れないことをお勧めします。さらに、オンライン ファブリックの同時分析の実行時間に悪影響を与えるリスクを回避するために、新しい分析を作成する前に少し（約 10 分）待つことをお勧めします。

  差分分析によってデータベースの負荷が増加するため、相互依存が発生します。複数の連続した差分分析によりデータベースの負荷が高い状態が維持されると、オンライン分析の実行時間に影響を与える可能性があります。

- **APIC** 構成エクスポート ポリシーは、両方のスナップショットで同じフォーマット（XML/JSON）で

表示されます。

- APIC 設定エクスポートポリシーの収集エラーがある場合、ポリシーの差分は実行されません。
- 表示される結果から承認済みの異常をフィルタできる［承認済みの異常を含める（Include Acknowledged Anomalies）］のトグルでは、手動で承認済みの異常は表示されません。

デルタ分析を作成

ACI アシュアランス グループ ユーザーの場合、APIC 管理者の writePriv 権限により、APIC ホストとリーフスイッチで情報を収集できます。**APIC** 設定エクスポートポリシーを構成するには、APIC 管理者の writePriv 権限が必要です。

[分析（**Analyze**）**]** > **[**分析ハブ（**Analysis Hub**）**]** > **[**差分分析（**Delta Analysis**）**]** > **[**差分分析の作成（**Create Delta Analysis**）**]** を選択します。

1. **[**差分分析の 名前（**Delta Analysis Name**）**]** フィールドに、名前を入力します。名前は、すべての分析で一意である必要があります。
2. **[**ファブリック（**Fabric**）**]** をクリックして、ファブリックを選択します。
3. **[**前のスナップショットの選択（**Choose Earlier Snapshot**）**]** をクリックし、差分分析の最初のスナップショットを選択します。[適用（Apply）] をクリックします。
4. **[**後のスナップショットの選択（**Choose Later Snapshot**）**]** をクリックし、差分分析の 2 番目のスナップショットを選択します。クリックします。
   [適用**]**をクリックします：

   デルタ分析用に選択した 2 つのスナップショットは、同じファブリックに属している必要があります。

5. **[**概要（**Summary**）**]** で作成された差分分析の概要をビューします。
6. [保存（Save）] をクリックします。デルタ分析のステータスは、**[**デルタ分析（**Delta Analysis**）**]** テーブルに表示されます。完了後、**[**差分分析の表示（**View Delta Analysis**）**]** または **[**別の差分分析の作成（**Create another Delta Analysis**）**]** を実行できます。

一度に 1 つの差分分析を実行できます。別の差分分析を実行するには、現在の差分分析を停止してから、別の差分分析を開始する必要があります。

1. (任意) [ステータス（Status）] 列から、進行中またはスケジュールされた分析を選択し、**[...]** オプションの
   [停止（STOP）] をクリックして差分分析を停止します。
2. **[...]** をクリックすると、作成した分析を 削除できます。

差分ルールの作成中にエラーが発生した場合は、ルール作成の概要にバナーとして表示されます。

デルタ分析の表示

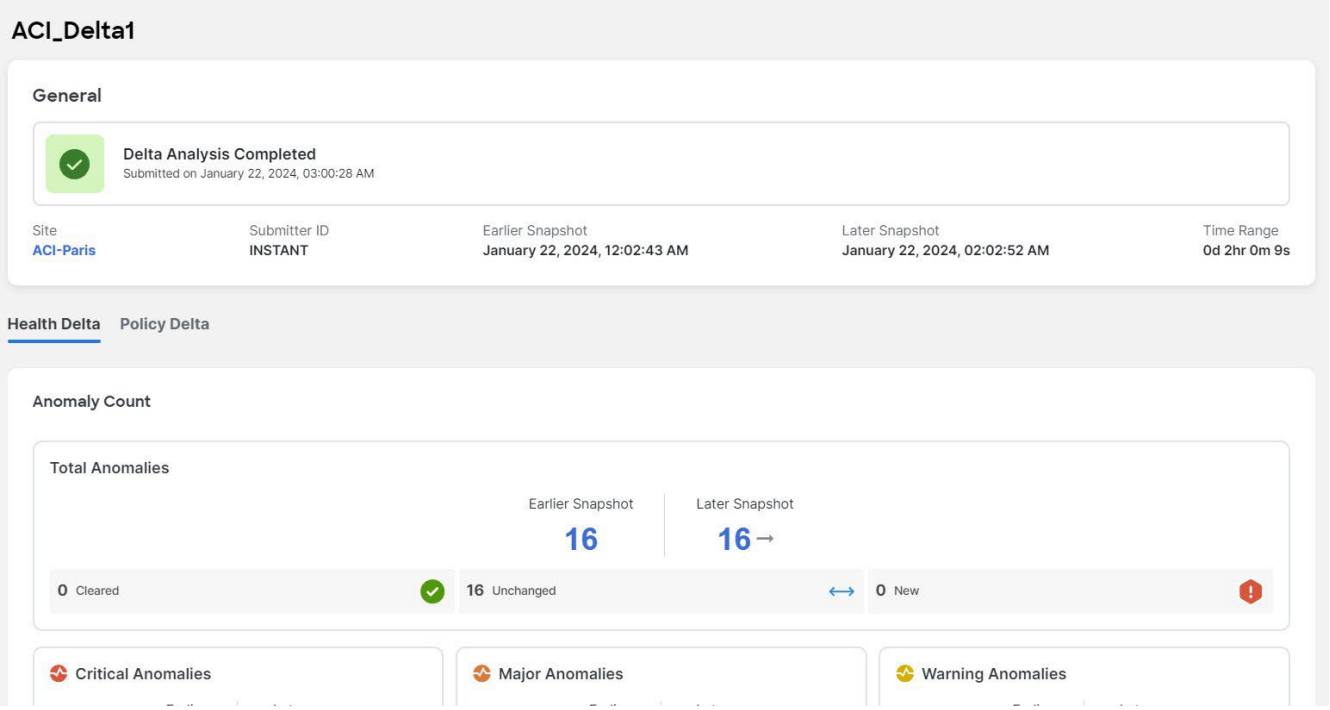
このページには、分析が表形式で表示されます。分析はステータスでソートされています。**[**差分分析の作成（**Create Delta Analysis**）**]** ボタンを使用すると、新しい差分分析を作成できます。

分析のステータスは、**[**中断（**Aborted**）**]**、**[**保留中（**Pending**）**]**、**[**停止済み（**Stopped**）**]**、**[**停止中（**Stopping**）**]**、**[**成功（**Success**）**]**、**[**失敗（**Failed**）**]**、**[**一部失敗（**Partially Failed**）**]**、**[**キュー済み（**Queued**）**]**、**[**完了（**Completed**）**]**、**[**進行中（**In progress**）**]** のいずれかになります。

フィルタ バーを使用すると、次の要因で分析をフィルタ処理できます。

- 名前
- ステータス
- Fabric)
- 送信者 ID

差分分析ダッシュボードには、分析の一般的な詳細が、正常性とポリシーの差分とともに表示されます。



- 正常性の差分分析の結果を表示するには、「正常性の差分分析の表示」を参照してください。
- ポリシーのデルタ分析の結果を表示するには、「ポリシーの差分分析の表示」を参照してください。

正常性の差分分析の表示

正常性の差分では、2 つのスナップショット間におけるファブリックの正常性の違いを分析します。結果は次のエリアに表示されます。

[承認済みの異常を含める（Include Acknowledged Anomalies）] のトグルをオンにすると、承認済みの異常を表示結果から除外することができます。無効な場合、手動で承認された異常は [異常カウント（Anomaly Count）] に含まれます。

- **[異常数（Anomaly Count）]**：スナップショット全体の重大度ごとに異常数の差が表示されます。表示される違いをクリックすると、**[すべての異常（All Anomalies ）]** テーブルがそれに応じてフィルタリングされます。

最初の数は、以前のスナップショットでのみ見つかった異常数を表します。2 番目の数は、両方のスナップショットに共通する異常数を表します。3 番目の数は、後のスナップショットでのみ見つかった異常数を表します。

- **[リソース別の正常性の差分]**：正常性に変化が見られたリソースの数がタイプ別に表示されます。**[変更を表示（View Changed）]** チェックボックスをオンにして、正常性が変更されたリソースを表示することもできます。歯車アイコンを使用すると、ビューごとに列をカスタマイズできます。フィルタ

バーは、「リソース」でテーブル内のリソースをフィルタするのに役立ちます。

テーブルには、カウント差分と正常性差分が表示されます。カウント差分には、正常なリソースと異常なリソースの両方が含まれます。フィルタ処理された正常性差分には正常でないリソースのみが表示され、

- **[**すべての異常（**All Anomalies**）**]** : **[**グループ化（**Grouped**）**]** ビューには、2 つのスナップショット間で集約された異常の差分ステータスが表示されます。**[**グループ解除（**Ungrouped**）**]** ビューには、2 つのスナップショット間における異常ごとの差分ステータスが表示されます。

異常は、次の種類のスナップショットについてリスト化できます。

- 以前のスナップショット
- 後のスナップショット
- 以前のスナップショットのみ
- 後のスナップショットのみ
- 両方のスナップショット

異常が以下のフィールドで表形式で表示されます。

- タイトル
- 異常レベル
- カテゴリ
- 数

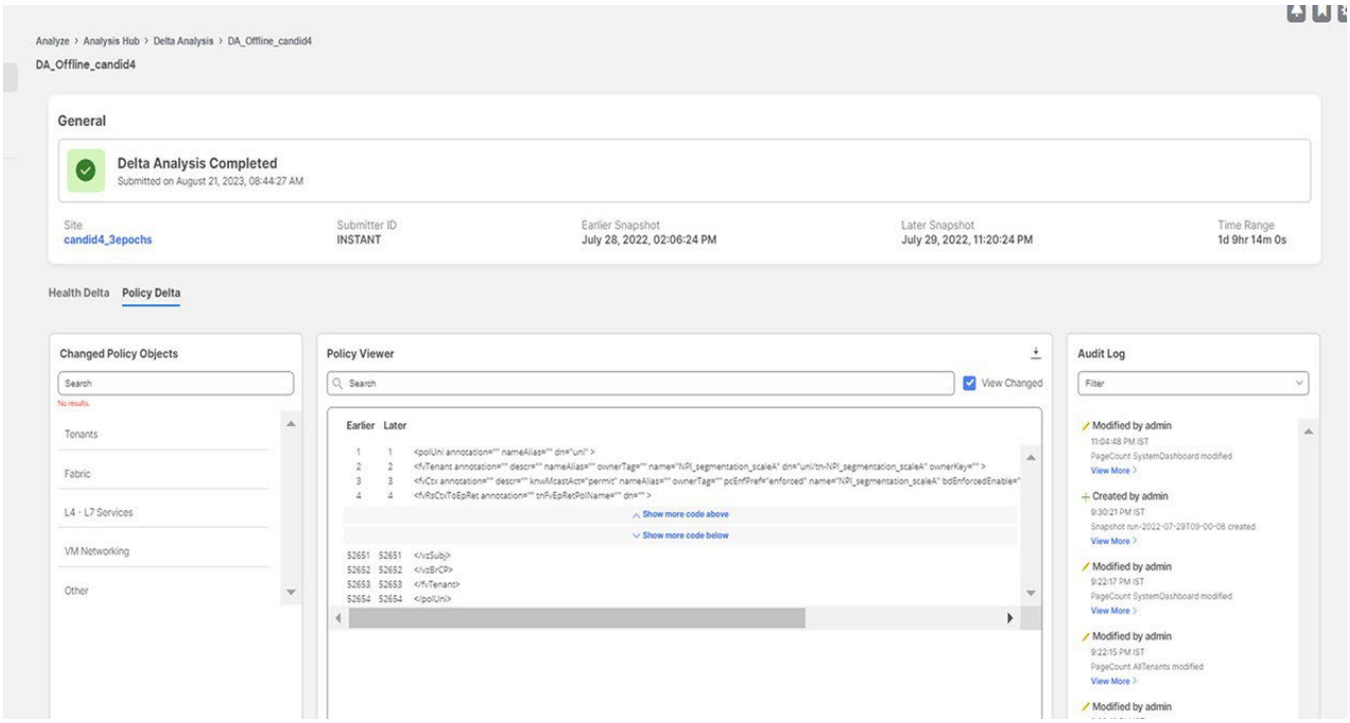
歯車アイコンを使用すると、ビューごとに列をカスタマイズできます。

次の属性に基づいて結果をフィルタできます。

- 異常レベル
- アプリケーション プロファイル DN
- BD DN
- タイトル
- コントラクト DN
- EPG
- 外部ルート
- インターフェイス
- 内部サブネット
- L3Out DN
- リーフ DN
- テナント DN
- エンドポイント
- VRF DN

異常を選択し、異常の詳細を表示します。

ポリシー差分分析の表示



[ポリシーの差分（**Policy Delta**）] をクリックして、2 つのスナップショット間におけるポリシーの変更を表示します。ポリシーの差分には、[変更されたポリシー オブジェクト（Changed Policy Object）]、[ポリシー ビューア（Policy Viewer）]、および [監査ログ（Audit Log）] の 3 つのセクションが含まれています。

1. **[変更されたポリシー オブジェクト（Changed Policy Object）]** パネルには、2 つのスナップショット間で変更されたポリシー オブジェクト ツリーが表示されます。[ポリシービューア]および[監査ログ]パネルでは、対応する変更が強調表示されます。**[検索]** バーを使用して、DN 検索を実行します。
   a. 特定のオブジェクトをドリルダウンして、変更されたオブジェクトタイプを表示します。数字は、オブジェクトに対する変更の数を示します。
   b. 変更されたオブジェクト タイプを選択して、変更された異常を表示します。
   c. [DN]リンクをクリックして、APIC で影響を受けるオブジェクトタイプにアクセスします。
   d. **[変更の表示（Show Changes）]** をクリックして、[ポリシービューア（Policy Viewer）] および [監査ログ（Audit Log ）] パネルに変更を表示します。
2. **[ポリシービューア（Policy Viewer）]** パネルには、以前のスナップショットと後のスナップショットにわたるポリシー構成が表示されます。また、2 つのスナップショット間で追加、変更、および削除されたポリシー構成を表示し、ポリシー差分の変更されたエリアに関するコンテキストを表示するのにも役立ちます。
   a. カラーコードを使用して、2 つのポリシー間で追加、削除、変更されたコンテンツ、および変更されていないコンテンツを可視化します。
   b. より多くのコンテンツを表示するには、**[**上に追加のコードを表示**]**または**[**下に追加のコードを表示**]** をクリックします。
   c. ダウンロード アイコンをクリックし、以前のスナップショットポリシーと後のスナップショットポリシーのポリシー構成をエクスポートします。
   d. **[検索（Search）]** バーに値を入力し、ポリシー差分の追加、変更、削除、変更されていないエリアのテキスト検索を実行します。
3. **[監査ログ（Audit Log）]** パネルには、2 つのスナップショット間で作成されたすべての監査ログが表示されます。Cisco Nexus Dashboard Insights は、APIC から監査ログを収集し、2 つのスナップショット間の監査ログの違いを計算します。

データセンターで変更された内容の相関ビューが **[**監査ログ（**Audit Log**）**]** パネルに表示されます。[変更された

ポリシー オブジェクト（**Changed Policy Objects**）**]** パネルで特定のオブジェクトを選択すると、関連する相違点が **[**ポリシー ビューア（**Policy Viewer**）**]** パネルで強調表示され、関連する監査ログが **[**監査ログ（**Audit Log**）**]** パネルで強調表示されます。APIC 監査ログは、監査可能である必要があるログインとログアウトや設定の変更など、ユーザーが開始したイベントのレコードです。すべてのスナップショットについて、監査ログの履歴は過去 24 時間までに制限されています。

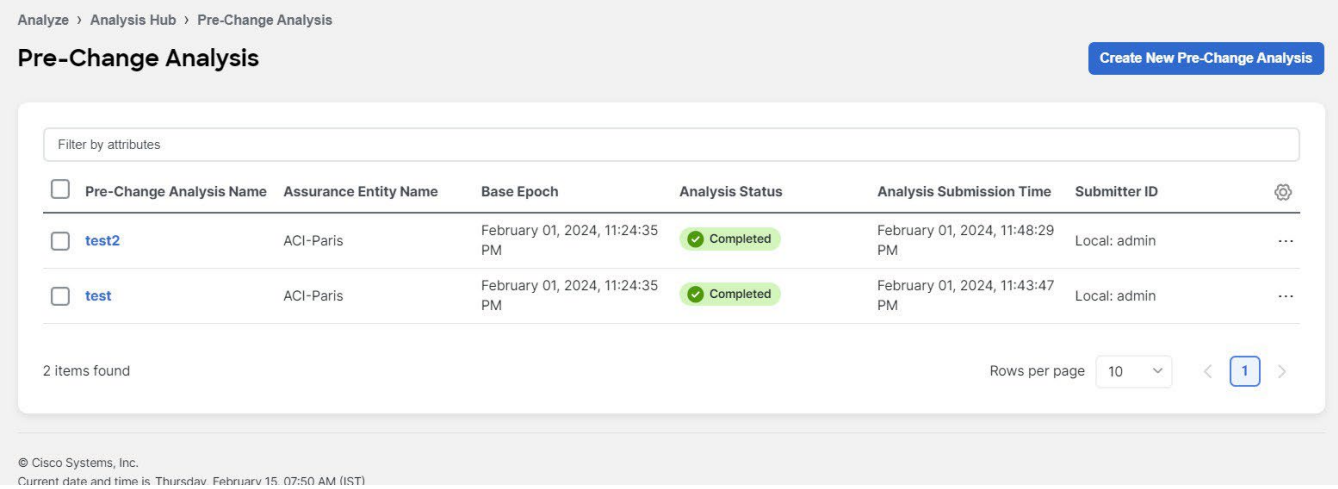
a. **[**フィルタ（**Filter**）**]** バーを活用して、DN、ユーザー識別子 、または任意でフィルタ処理します。
b. 監査ログ エントリで **[**詳細を表示（**View More**）**]** をクリックして、変更時刻と変更者を表示します。監査ログエントリのタイムスタンプは、APIC 監査ログのタイムスタンプに対応します。
c. [監査ログ]エントリをクリックして、APIC で影響を受けるオブジェクトタイプにアクセスします。

変更前

変更前の分析

[分析（Analyze）] > [分析ハブ（Analysis Hub）] > [変更前（Pre-Change）] の順に選択します。

[変更前分析（Pre-Change Analysis）] では、ファブリックの構成を変更し、意図した変更をモデル化し、サイト内の既存の基本スナップショットに対して変更前の分析を実行し、その変更で目的の結果が生成されるかどうかを確認できます。

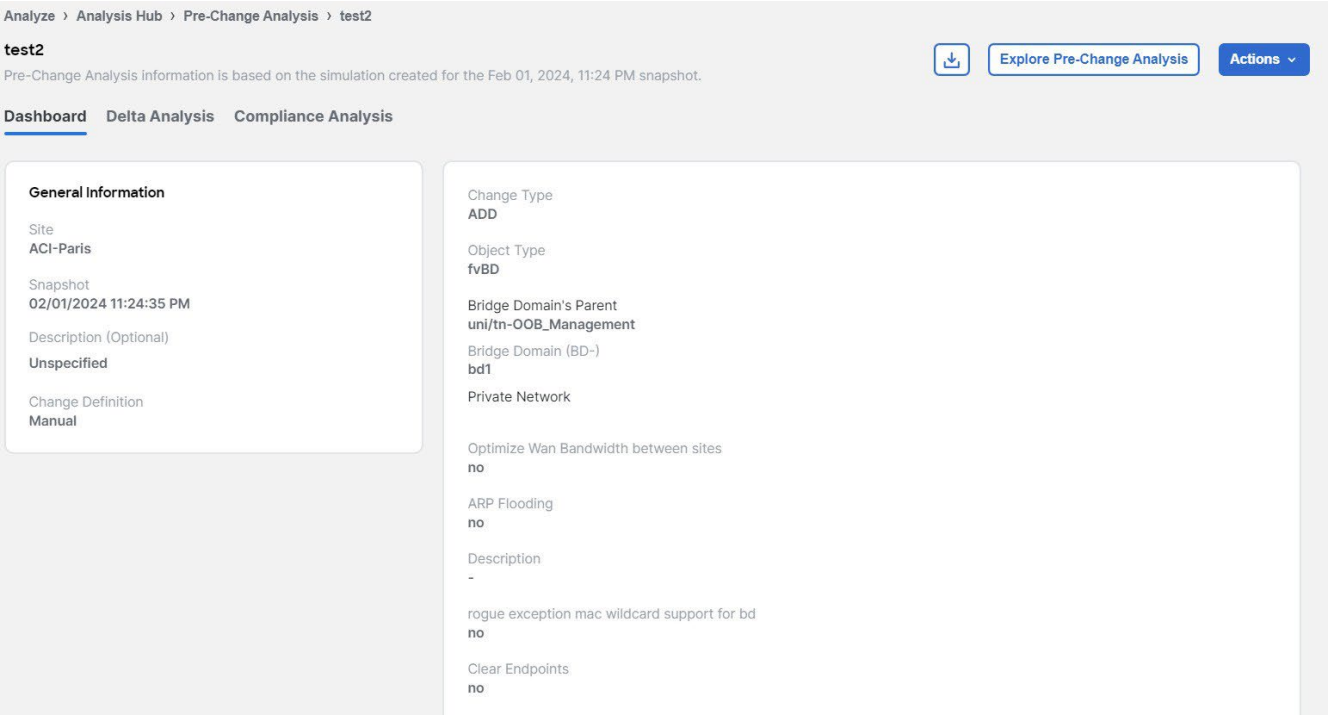


変更前の分析ジョブに対する変更をモデル化したら、**[保存（Save）]** または **[保存して分析（Save And Analyze）]** を選択できます。**[保存（Save）]** を選択すると、すぐに分析を開始しなくても、変更前の分析ジョブを保存できます。後でジョブに戻り、必要に応じて変更を編集し、分析を実行できます。**[保存（Save）]** オプションは、手動で変更した変更前の分析ジョブでのみサポートされています。

[保存して分析（Save And Analyze）] を選択すると、ジョブがスケジュールされ、分析が提供されます。変更は選択されたベース スナップショットに適用され、分析が実行され、結果が生成されます。表にリストされているすべての変更前の分析ジョブについて、基本スナップショットと新たに生成されたスナップショットの間で差分分析が実行されます。

[変更前の分析（Pre-Change Analysis）] で、完了した変更前の分析ジョブの詳細を表示するには、テーブル内のそのジョブをクリックします。これにより、次の情報を表示する新しいページが開きます。

- ダッシュボード
- デルタ分析
- コンプライアンス分析



[一般情報（General Information）] には、次のデータが表示されます。

- ファブリック名
- スナップショットの詳細
- 説明
- 定義の変更

手動変更の場合は、そのジョブ用にモデル化された変更（変更タイプ、オブジェクト タイプ、名前エイリアス、優先度、説明、アプリケーション プロファイル）のリストが表示され、JSON/ XML ファイルのアップロードの場合は、変更シミュレーションが表示されます。

ジョブが完了すると、[重大度]領域に、それらの変更に対して生成された異常が表示されます。[差分分析（Delta Analysis）] に表示されるデータを理解するには、[差分分析（DeltaAnalysis）] を表示します。

[コンプライアンス分析（Compliance Analysis）] に表示されるデータを理解するには、

[コンプライアンス（Compliance）] を参照してください。**[...]** ボタンを使用すると、

次のアクションを実行できます。

- 変更前分析の編集
- 変更前分析の複製
- 変更前分析の削除

これらのアクションは、目的のジョブのチェックボックスをクリックするか、
[アクション（Actions）] ボタンを使用してこれらのアクションを実行することもできます。

次の 3 つのアクションを実行する際の注意事項：

1. 手動変更の場合のみ、変更前の分析ジョブを複製できます。
2. 一度に最大 10 個の変更前の分析ジョブを削除できます。[実行中（Running）] 状態のジョブを

削除できません。削除しようとすると、適切な通知が表示されます。

分析で異常が発生した場合は、結果に基づいて必要な修正を加え、満足のいく結果が得られるまで分析を再実行します。変更前の分析ジョブのダウンロードオプションを使用すると、Cisco APIC にアップロードできる JSON ファイルをダウンロードできます。ただし、ファイル アップロード アプローチを選択した場合は、JSON または XML Cisco APIC 構成ファイルをアップロードして、変更前の分析ジョブを実行できます。

分析が開始されると、ジョブのステータスは[実行中]と表示されます。この間、指定された変更は基本スナップショットの上にモデル化され、ポリシー分析とコンプライアンスを含む完全な論理チェックが実行されます。スイッチソフトウェアまたは TCAM のチェックは実行されません。差分分析を含む分析全体が完了すると、変更前の分析ジョブのステータスが **[**完了（**Completed**）**]** とマークされます。差分分析が自動的にトリガーされ、関連する変更前の分析ジョブがその間 [実行中（Running）] として表示されます。差分分析は、変更前の分析ジョブでサポートされているチェックに対してのみ実行されます。

テーブルでジョブをクリックすると、特定の [変更前の分析（Pre-Change Analysis）] ジョブにユーザーが適用した変更を表示できます。変更を手動で適用すると、ユーザーが選択したさまざまな変更を表示できます。ジョブが JSON ファイルを使用して作成されている場合、[変更定義（Change Definition）] フィールドに、変更のインポート元の JSON ファイルの名前が表示されます。

[変更前分析（Pre Change Analysis）] には、実行されたすべての分析が次のフィールドを含む表形式で一覧表示されます。

1. 分析名
2. アシュアランスエンティティ名
3. 基本エポック
4. 分析ステータス
5. 送信者 ID

変更前の分析オプション

次のリストは、変更前の分析ジョブに選択できるオプションを指定します。リストされているオブジェクトのみサポートされています。

1. テナントを追加、変更、または削除します。
2. アプリ EPG を追加、変更、または削除します（*サポートされている属性：*優先グループメンバー、EPG 内分離、*アプリ EPG の関係*: BD、提供、消費、タブー コントラクト。コントラクトの*エクスポート*/インポートはサポートされていません）。
3. VRF を追加、変更、または削除します（*サポートされている属性*: ポリシー コントロールの適用設定、ポリシー コントロールの適用方向、BD 適用ステータス、優先グループ メンバー、説明）。
4. BD を追加、変更、または削除します（*サポートされている属性*：説明、WAN 帯域幅の最適化、タイプ、ARP フラッディング、IP ラーニング、IP ラーニングをサブネットに制限、L2 不明ユニキャスト、ユニキャスト ルーティング、マルチ宛先フラッディング、マルチキャスト許可、L3 不明マルチキャスト フラッディング）。
5. 契約を追加、変更、または削除します（*サポートされている属性*：スコープ、説明)。
6. コントラクト サブジェクトを追加、変更、または削除します（*サポートされている属性*：リバース フィルタ ポート、説明、優先順位、ターゲット DSCP、フィルタ名、転送フィルタ名、リバース フィルタ 名 ）。

7. サブネットを追加、変更、または削除します（*サポートされている属性*：スコープ、優先、説明、プライマリ IP アドレス、仮想 IP アドレス、サブネット コントロール）。
8. アプリプロファイルを追加、変更、または削除します(優先順位、説明)。
9. L3Out を追加、変更、または削除します（*サポートされている属性:*：説明、VRF 名、ターゲット DSCP、ルート制御適用）。
10. L2Out を追加、変更、または削除します（*サポートされている属性*：説明、BD 名、カプセル化タイプ、カプセル化 ID）。
11. L3 Ext EPG を追加、変更、または削除します（*サポートされている属性*：優先グループ メンバー、説明、優先順位、*サポートされている関係*：VRF、提供されたコントラクト、消費されたコントラクト、タブー、ターゲット DSCP）。
12. L2 Ext EPG を追加、変更、または削除します（*サポートされている属性*：優先グループメンバー、説明、優先順位、ターゲット DSCP および提供されたコントラクト、サポートされているコントラクト、タブーコントラクト）。
13. L3 Ext EPG サブネットを追加、変更、または削除します（*サポートされている属性*：説明、範囲）。
14. タブー コントラクトを追加、変更、または削除します（*サポートされている属性*：説明）。
15. タブー サブジェクトを追加、変更、または削除します（*サポートされている属性*：名前、説明、*サポートされている関係*：vzRsDenyRule）。
16. フィルタ、フィルタエントリを追加、変更、および削除します。

ファブリック アクセス ポリシーの場合、変更前の分析ジョブに以下の内容を追加できます。

1. EPG と物理ドメイン間の関係を追加、変更、または削除します。
2. 物理ドメインと対応する VLAN プール間の関係を追加、変更、または削除します。
3. 物理ドメインと接続可能なエンティティプロファイル間の関係を追加、変更、または削除します。
4. リーフ インターフェイス プロファイルを追加、変更、または削除します。
5. ポートセレクタを追加、変更、または削除します。
6. スイッチプロファイルを追加、変更、または削除します。
7. スイッチセレクタを追加、変更、または削除します。
8. インターフェイス ポリシー グループを追加、変更、または削除します。
9. CDP および LLDP のインターフェイスポリシーを追加、変更、または削除します。

変更前の注意事項および制限事項

変更前の分析を使用する場合は、次のガイドラインと制約事項に従ってください。

- ファブリックおよびアップロードされたファイルに対して変更前の分析を実行できます。
- 同じ基本スナップショットで複数の変更前の分析を実行できます。
- 変更前の分析は、基本スナップショットとして使用されている変更前のスナップショットに対しては実行できません。
- 論理構成の異常のみがモデル化され、変更前の分析で実行されます。スイッチソフトウェアと TCAM の変更はモデル化されていません。分析が完了すると、差分分析が自動的に開始され、変更前の分析によって生成されたスナップショットと基本スナップショットが比較されます。差分分析は、変更前の分析ジョブでサポートされているチェックに対してのみ実行されます。

- 変更前の分析中、基本スナップショットに存在する特定の異常は、変更前の分析では分析されません。その結果、違反が引き続き存在する場合でも、それらの異常は変更前の分析スナップショットには表示されません。そのようなイベントが変更前の分析で分析されない理由は、それらの異常の分析には論理データだけでなく、スイッチソフトウェアと TCAM データも必要だからです。
- コンプライアンス分析には、変更前の分析スナップショットのコンプライアンスチェックの結果が表示されます。
- 変更前の分析スナップショットから異常のローカル検索を実行し、**[**ダッシュボード（**Dashboard**）**]**、**[**差分分析（**Delta Analysis**）**]**、**[**コンプライアンス分析（**Compliance Analysis**）**]**、および **[Explore]** の特定のタブに移動して、結果セクションに表示します。
- 変更前の分析では、サービスチェーンに関連する変更やオブジェクトはサポートも分析もされません。
- [差分分析（Delta Analysis）] では、変更前の分析スナップショットを選択できません。
- 構成スナップショットの設定データが存在しない場合に、このスナップショットを使用して変更前の分析ジョブを実行すると、新しい論理構成ファイルは生成されません。このような変更前の分析ジョブの場合、[ダウンロード（Download）] アイコンはサイドパネルでグレー表示または無効になります。新しい論理構成をダウンロードすることはできません。
- インポートされた構成にサポートされていないオブジェクトが含まれている場合、変更前の分析は [失敗（Failed）] 状態になる可能性があります。「変更前の分析オプション」セクションを参照してサポートされていない Cisco ACI オブジェクトを特定し、削除して、構成を再度インポートしてから、別の変更前の分析ジョブを開始します。失敗した変更前の分析がある場合、失敗のエラー メッセージが **[**分析ステータス（**Analysis Status**）**]** の [変更前の分析（Pre-Change Analysis）] テーブルに表示されます。
- 変更前の分析機能は、Cisco APIC リリース 3.2 以降でサポートされています。リリース 3.2 より前の Cisco APIC リリースで変更前の分析を実行しようとすると、変更前の検証は APIC 3.2 以降でサポートされていることを示すエラーメッセージが表示され、分析を実行できません。
- 変更前の分析の開始時に現在実行中の分析がある場合、実行中のジョブが最初に完了します。新しいジョブはスケジュールされた順序で処理されます。Cisco Nexus Dashboard Insights は、スケジュールと使用可能なリソースに最適な順序でジョブを実行します。変更前の分析ジョブを含むすべてのジョブには、同じ優先順位が与えられます。
- JSON または XML Cisco APIC 構成ファイルをアップロードして、変更前の分析ジョブを実行できます。
  - ファイルの最大サイズは、vND の場合は 10 MB、pND の場合は 50 MB です。
  - アップロードされたファイルは、ファイルサイズを削減するために空白とエンドポイントオブジェクト（FvCEP）を削除することによってプルーニングされます。
- 変更前分析ジョブは、必要な数だけ保存できます。ただし、ファブリックの場合、変更前分析ジョブは一度に 1 つしか実行できません。
- テナントに属するオブジェクトを変更する場合、そのテナントの変更前の分析ファイルのサイズは 10 MB を超えることはできません。

変更前の分析における複数オブジェクトのサポート

複数のテナントに加えて、変更前の分析の JSON または XML ジョブの一部として複数のインフラストラクチャ オブジェクトを追加することもできます。変更前の分析のアップロードパスを使用すると、ポリシーユニバース全体で複数のオブジェクトを追加、変更、および削除できます。この機能を使用するために必要な追加の設定はありません。アップロードしたファイルに基づいて、複数オブジェクトの変更前の分析ジョブが実行されます。

次のファイルアップロード形式を使用できます。

- サイズが 1 の IMDATA を含む JSON または XML ファイル。
- 意図した変更の単一のサブツリーを含む IMDATA。サブツリーのルートは、変更が単一のサブツリーとして表される限り、UNI または他の管理対象オブジェクトにすることができます。
- JSON または XML パスからアップロードしたファイルを使用して、変更前の分析を実行します。変更前の分析が完了したら、同じファイルを ACI にアップロードして、変更に使用できます。

変更前の分析に関する既知の問題

- 変更前の分析のスケール制限を超えると、エラーメッセージが表示されずに分析が失敗する可能性があります。
- 変更前の分析ジョブでは、EPG、BD、VRF の総数が 16,000 を超える設定を変更しないでください。
- 新しい変更前の分析を作成するときは、次の点に注意してください。
  - アップロードされる JSON/XML ファイルのサイズが 100 MB 未満で 15 MB を超える場合、API がファイルを検証し、「*アップロードファイルのサイズが 15MB(pND)/8MB(vND) の上限を超えています（Uploaded file size exceeds the 15MB(pND)/8MB(vND) maximum limit.）」のような検証エラーがスローされます。*ユーザーが Cisco Nexus Dashboard Insights にアクセスし、15MB(pND)/8MB(vND) を超えるファイルサイズで変更前の分析ジョブを作成しようとすると、「*ファイル サイズは 15MB(pND)/8MB(vND) を超えることはできません（File size cannot be larger than 15MB(pND)/8MB(vND).）*」というエラーが UI からスローされます。したがって、15MB(pND)/8MB(vND)を超えるファイルは変更前の分析ではサポートされていません。
  - サポートされていないオブジェクトを含むファイルをアップロードすると、Cisco Nexus Dashboard Insights はサポートされていないオブジェクトを削除し、ジョブを実行します。
- Cisco ACI 構成に Cisco Nexus Dashboard Insights でサポートされていない機能が含まれている場合、変更前の分析ジョブは失敗するか、誤った結果を返すことがあります。
- サービスチェーンを含む Cisco ACI 設定では、変更前の分析はサポートされていません。
- Cisco Nexus Dashboard Insights は、変更前の分析のためにアップロードされた JSON ファイルに対して限定された一連のチェックを実行します。Cisco ACI は、このファイルを拒否する場合があります。
- 変更前の分析では、外部ルーテッド ネットワークのサブネットの属性に関するエラーが誤って報告される場合があります。
- 変更前の分析は、次の Cisco APIC リリースでサポートされています。
  - 3.2(x)リリースでは、3.2(9h)以前がサポートされています。
  - 4.0(x)リリースでは、4.0(1h)以前がサポートされています。
  - 4.1(x)リリースでは、4.1(2x)以前がサポートされています。
  - 4.2(x) リリースでは、4.2(7s) 以前がサポートされています。
  - 5.0(x)リリースでは、5.0(2e)以前がサポートされています。
  - 5.1(x)リリースでは、5.1(4c)以前がサポートされています。
  - 5.2(x) リリースでは、5.2(4d) 以前がサポートされています。
  - 5.3(x) リリースでは、5.3(1b) 以前がサポートされています。
  - 6.0(x) リリースでは、6.0(4c) 以前がサポートされています。

変更前の分析ジョブの作成

1. **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[変更前（Pre-Change）]** の順に選択します。
2. **[変更前（Pre-Change）]** ページで、**[変更前の分析の作成（Create Pre-Change Analysis）]** の順に選択します。**[変更前の分析の作成（Create Pre-Change Analysis）]** で、次の操作を実行します。

全般

a. **[変更前の分析名（Pre-Change Analysis Name）]** フィールドに、名前を入力します。

b. 必要な場合は、**[説明（Description）]** フィールドに、タグの説明を追加します。

c. **[ファブリック（Fabric）]** フィールドで、適切なファブリックを選択します。

d. **[スナップショット（Snapshot）]** フィールドで、適切なスナップショットを指定します。

変更

a. **[変更（Change）]** で、適切なオプションを選択します。（**[JSON/XML ファイルのインポート（Import JSON/XML File）]** または **[手動変更（Manual Changes）]**）。

選択内容に応じて、入力する関連フィールドが表示されます。

JSON または XML ファイルをアップロードするファイル インポート オプションを選択した場合は、**[保存して実行（Save & Run）]** をクリックして、変更前の分析操作を開始する必要があります。

手動変更オプションを選択した場合は、**[Change Type]** および **[Object Type]** を選択し、ジョブを保存または実行するか、ジョブを保存して、**[アクション（Actions）]** > **[変更前の分析の編集（Edit Pre-Change Analysis）]** をクリックして、**[保存して実行（Save & Run）]** をクリックして後で開始できます。**[編集（Edit）]** では、必要に応じて一部のフィールドを変更することもできま

必要に応じて選択を完了し、**[保存（Save）]** または **[保存して実行（Save & Run）]** をクリックします。

変更前の分析ジョブが完了すると、**[変更前の分析（Pre-Change Analysis）]** テーブルにジョブのステータスが [完了（Completed）] として表示されます。

詳細を表示する変更前の分析名をクリックします。右側のサイドバーでは、ジョブの名前、スナップショット、変更定義タイプなどの一般情報を含む列に詳細が表示されます。ジョブ用にモデル化された変更のリストも使用できます。完了したジョブを表示している場合は、変更の結果として生成された異常がこのページの上部に表示されます。

完了したジョブの場合は、サイドバーの右上にあるアイコンをクリックして、結果ページに移動します。ジョブの詳細は、**[ダッシュボード（Dashboard）]**、**[差分分析（Delta Analysis）]**、**[コンプライアンス分析（Compliance Analysis）]**、特定のタブの下に表示されます。

変更前の分析ジョブのダウンロード

次の手順で、既存の変更前の分析をダウンロードできます。

- **[変更前の分析（Pre-Change Analysis）]** テーブルで、完了した変更前の分析ジョブの適切な変更前の分析名をクリックします。ファイルをダウンロードするには、ダウンロード アイコンをクリックします。

- 変更前の分析は、JSON 形式で表示される変更前の分析コンテンツを含むオフライン tar ファイルとしてダウンロードされます。

ダウンロードしたファイルでは、変更された属性と変更されていない属性を含むすべての属性を表示できます。必要に応じて、ダウンロードしたファイルを Cisco APIC にアップロードできます。

バグスキャン

バグスキャン

Nexus Dashboard Insights は、すべてのデバイスからテクニカル サポート情報を収集し、既知の署名セットに対して実行し、対応する欠陥と PSIRT にフラグを立てます。Nexus Dashboard Insights は、PSIRT のアドバイザリと欠陥の異常も生成します。メタデータのサポートの詳細については、「異常およびアドバイザリ」を参照してください。

バグ スキャン機能は、ファブリック内のデバイスからテクニカル サポート ログを収集し、ヒットした可能性のあるバグをスキャンします。CPU およびメモリの使用状況が設定されたしきい値 65% 以下であれば、テクニカル サポートのログが収集され、デバイスのバグ スキャンが実行されます。CPU およびメモリの使用状況が設定されたしきい値を超えている場合、そのデバイスはバグ スキャンから除外され、最終的に次のデフォルトのバグ スキャン、またはそのデバイスのオンデマンド バグ スキャンを実行する際に再検討されます。

デバイスのノードの相互作用が正常でない場合、ログ収集のためにバグスキャンを実行するデバイスを選択できません。ジョブを構成するデバイスを選択できません。

ファブリックのオンデマンドバグ スキャンを実行することもできます。詳細については『スタートアップガイド』の「オンデマンド分析」を参照してください。

デフォルトのバグスキャン

バグ スキャンは、Nexus Dashboard Insights にオンボーディングされたすべてのファブリックに対して実行され、各デバイスに対して 7 日ごとに自動スケジュールされます。このスケジュールは固定されており、カスタマイズできません。

バグ スキャンは、前回のバグ スキャン、またはバグ スキャンが以前に実行されていない場合はオンボーディング時間に基づいて、ファブリックに含まれるデバイスで実行されます。最後のバグ スキャンからの経過時間が長いデバイスが優先されます。デバイスでバグ スキャンが実行されると、成功したか失敗したかにかかわらず、次の 7 日間は同じデバイスに対して別のバグ スキャンが実行されません。

バグ スキャンは、デバイスの CPU とメモリのメトリックがストリーミングされ、使用率が 65% 未満の場合にのみ、デバイスで実行するように自動スケジュールされます。

ただし、オンデマンド バグ スキャンは例外であり、自動スケジュールされた実行よりも優先され、ユーザーが開始するため、CPU とメモリのメトリックは考慮されません。自動スケジュールされたベスト プラクティスが進行中であり、オンデマンドのベスト プラクティスが開始された場合、 Nexus Dashboard ノードで使用可能なリソースに基づいて、現在のベスト プラクティスが進行中または現在のベスト プラクティスの完了後にオンデマンドのベスト プラクティスが開始されます。

特定のデバイスで実行できるバグ スキャンは一度に 1 つだけです。ただし、バグ スキャンがすでに進行中の 1 つのデバイス セットがある場合、2 番目の（自動スケジュールまたはオンデマンドの）バグ スキャンは、Nexus Dashboard Insights に十分なリソースがある場合にのみ実行できます。それ以外の場合は、リソースが使用可能になるとすぐに保留され、開始されます。

バグ スキャンは、次のシナリオで自動的にトリガされます。

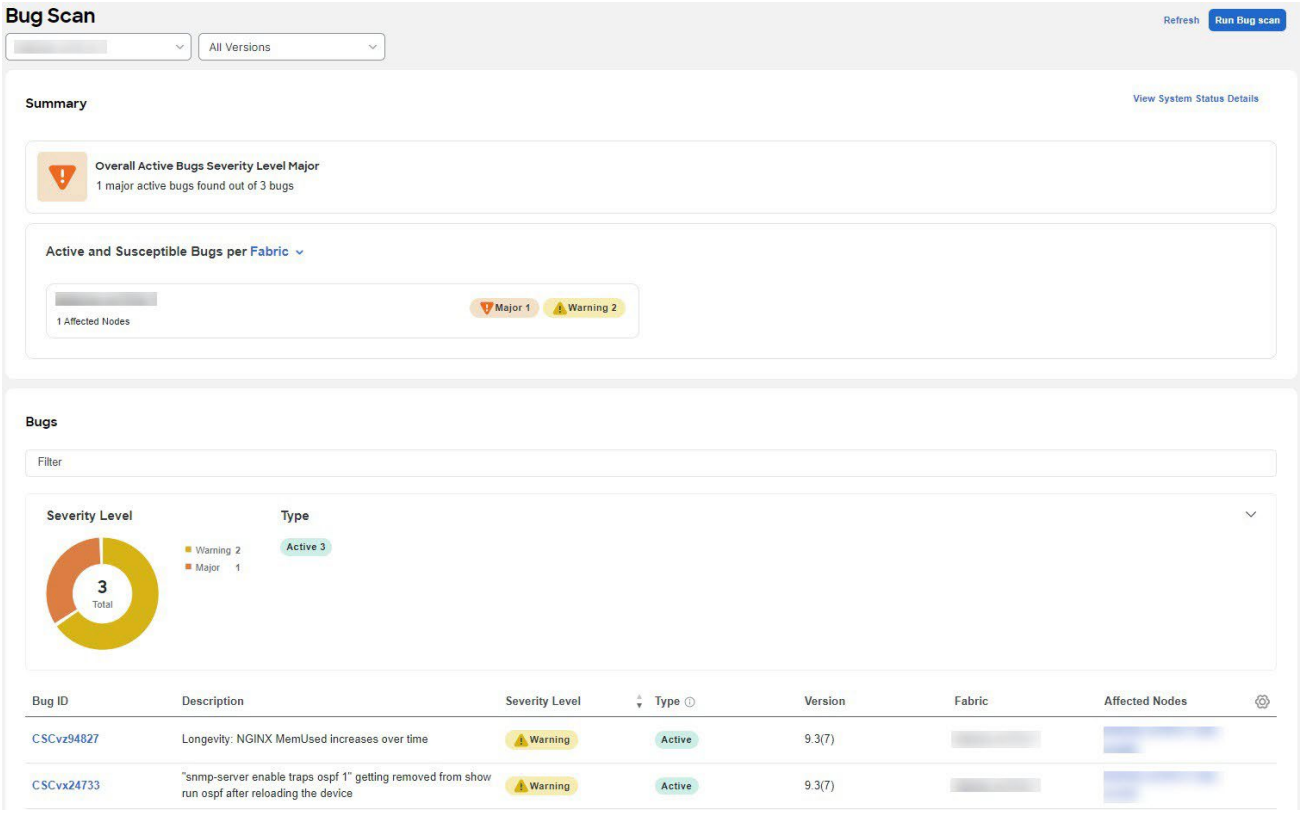
- アップグレードまたはダウングレード
- ノードのリロード

アクティブ バグと影響を受けやすいバグの表示

バグ スキャン機能は、ファブリック内のデバイスからテクニカル サポート ログを収集し、ヒットした可能性のあるバグをスキャンします。バグ スキャンの完了後に、ネットワークに影響を与えるアクティブ バグと影響を受けやすいバグを表示できるようになりました。

- [アクティブ バグ（Active Bugs）]：構成ファイルおよびテクニカル サポート ファイルに基づいてネットワークで検出された、バージョンに存在するバグ。
- [影響を受けやすいバグ（Susceptible Bugs）]：ネットワークに影響を与える可能性のある、バージョンに存在するバグ。

1. **[分析（Analyze）]** > **[分析ハブ（Analysis Hub）]** > **[バグ スキャン（Bug Scan）]** の順に選択します。
2. ドロップダウン メニューから、オンライン ファブリックまたは複数のオンライン ファブリックを選択します。
3. ドロップダウン メニューからソフトウェア バージョンを選択します。選択したファブリックとソフトウェア バージョンのアクティブ バグと影響を受けやすいバグが表示されます。



4. [概要（Summary）] エリアには、現用系バグ全体が重大度別に表示されます。ドロップダウン メニューを使用して、ファブリックまたはソフトウェア バージョンごとのバグを表示することもできます。
5. [バグ（Bugs）] エリアで、フィルタ バーを使用して、バグ ID、説明、重大度レベル、タイプ、および影響を受けるノードでバグをフィルタ処理します。
6. **[重大度レベル（Severity Level）]** の円グラフには、重大、主要、注意の重大度のバグの合計数が表示されます。
7. バグ テーブルを表示して、フィルタされたバグを確認します。
   a. 列の見出しをクリックして、テーブルのバグを並べ替えます。
   b. 歯車アイコンをクリックして、テーブルの列を構成します。

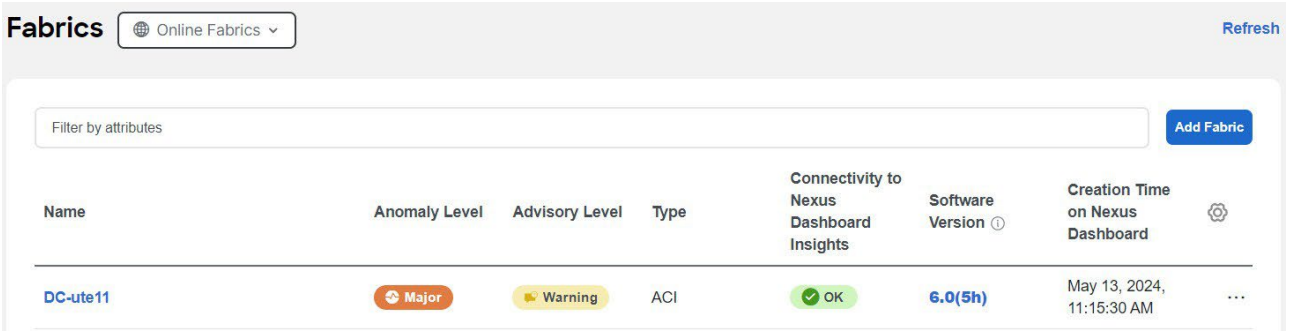
c. **[バグ ID （Bug ID）]** をクリックしてバグの詳細を表示します。

8. **[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンド バグ スキャンを実行します。ファブリックを選択し、**[今すぐ実行（Run Now）]** をクリックします。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

個々のファブリックのアクティブなバグと潜在的なバグのビュー

Nexus Dashboard Insights では、次の方法で個々のファブリックのバグを表示することもできます。

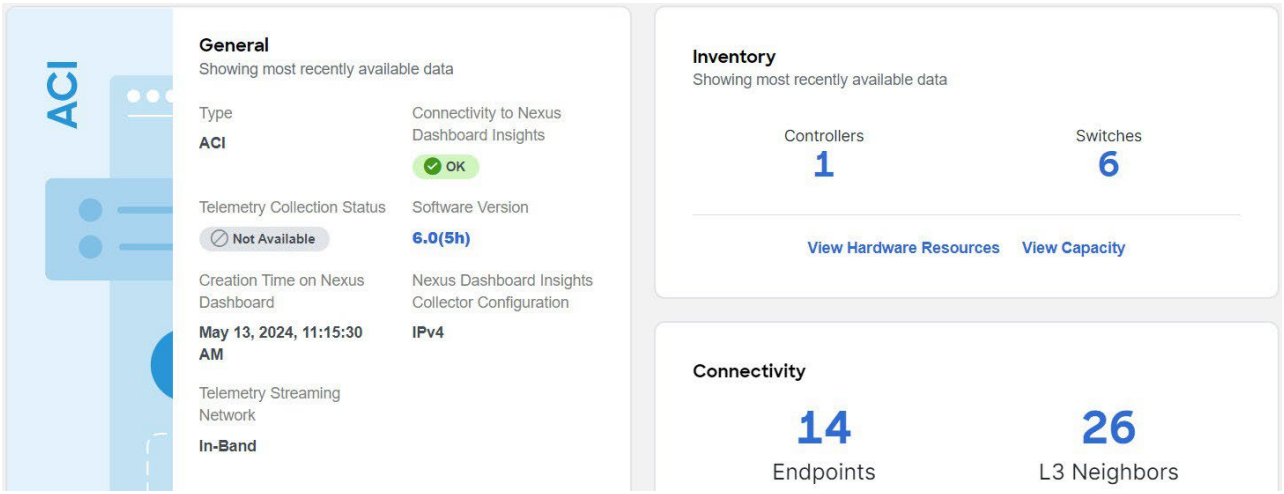
1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ドロップダウン メニューから **[オンライン ファブリック（Online Fabrics）]** を選択します。



3. ソフトウェア バージョン列で、ソフトウェア バージョンにカーソルを合わせ、**[バグの表示（View Bugs）]** をクリックして、そのファブリックのアクティブなバグと影響を受けやすいバグを表示します。
4. [アクション（Actions）] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** をクリックして、オンデマンドのバグ スキャンを実行します。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

または

1. **[管理（Manage）]** > **[ファブリック（Fabrics）]** に移動します。
2. ドロップダウン メニューから **[オンライン ファブリック（Online Fabrics）]** を選択します。
3. ファブリックを選択します。



4. [全般（General）] 領域で、ソフトウェア バージョンにカーソルを合わせ、**[すべてのバグの表示（View All Bugs）]** をクリックして、そのファブリックのアクティブなバグと影響を受けやすいバグを表示します。
5. [アクション（Actions）] ドロップダウンメニューから、**[バグ スキャンの実行（Run Bug Scan）]** を

クリックして、オンデマンドのバグ スキャンを実行します。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

または

1. **[**管理（**Manage**）**]** > **[**インベントリ（**Inventory**）**]** の順に選択します。
2. ドロップダウン メニューから **[**オンライン ファブリック（**Online Fabrics**）**]** を選択します。
3. [コントローラ（Controllers）] テーブルで、[ソフトウェア バージョン（Software Version）] 列のソフトウェア バージョンの上にマウスを合わせ、
   [バグの表示（**View Bugs**）**]** をクリックして、アクティブ バグと影響を受けやすいバグを表示します。
4. **[**スイッチ（**Switches**）**]** をクリックします。[スイッチ（Switches）] テーブルで、[ソフトウェア バージョン（Software Version）] 列のソフトウェア バージョンにカーソルを合わせ、**[**バグの表示（ **View Bugs**）**]** をクリックして、現用系バグと影響を受けやすいバグを表示します。
5. オンデマンドバグ スキャンを実行するには、[アクション（Actions）] ドロップダウンメニューから **[**バグ スキャンの実行（**Run Bug Scan**）**]** をクリックします。詳細については、『スタートアップ ガイド』の「オンデマンド分析」セクションを参照してください。

または

1. **[**管理（**Admin**）**]** > **[**ファブリック ソフトウェア管理（**Fabric Software Management**）**]** に移動します。
2. [ソフトウェア管理ジョブ（Software Management Jobs）] テーブルで、分析をクリックします。
3. [ファームウェアの概要（Firmware Summary）] エリアで、ノード ターゲット ファームウェアにカーソルを合わせ、**[**バグの表示（**View Bugs**）**]** をクリックして、そのファブリックのアクティブ バグと影響を受けやすいバグを表示します。
4. [アクション（Actions）] ドロップダウンメニューから、**[**バグ スキャンの実行（**Run Bug Scan**）**]** をクリックして、オンデマンドのバグ スキャンを実行します。詳細については『スタートアップ ガイド』の「オンデマンド分析」を参照してください。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Cisco および Cisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。